



COOK COUNTY GOVERNMENT

Office of the Chief Procurement Officer

Request for Proposal (RFP) No. 1912-17832

for

Food Service Management System

Proposals must be uploaded to:

<https://www.cookcountyil.gov/service/online-solicitation-bid-submission>

Proposals are due no later than 10:00 AM Central Standard Time on Wednesday, 1/13/2021

There will be a mandatory pre-proposal conference call

Tuesday, December 15, 2020 at 12:00 PM CST

https://teams.microsoft.com/l/meetup-join/19%3ameeting_ZjBiMDlkMzItZmVmZS00NTVILWFjZTI0NGVIYzVhMzk3MzBj%40thread.v2/0?context=%7b%22Tid%22%3a%228b4d55ae-6db4-4e05-a85c-59d6a256cd6e%22%2c%22Oid%22%3a%22099d9406-018d-414b-8e8e-8a1d089320f3%22%7d

There will be a mandatory site visit

Wednesday, December 16, 2020 - Times will be scheduled with each vendor

2750 S. California

Chicago, IL 60608

Questions regarding the RFP should be directed to:

Kelly Spencer, Buyer at Kelly.Spencer@cookcountyil.gov

Toni Preckwinkle
Cook County Board President

Raffi Sarrafian
Chief Procurement Officer

Food Service Management System RFP Table of Contents

1. Introduction	8
1.1. Background.....	8
1.2. Business Goals and Objectives.....	8
1.3. Schedule	9
1.4. Definitions	10
2. Scope.....	12
2.1. Detainee Meal Service.....	12
2.1.1 Detainee Meal Orders.....	12
2.1.2 Detainee Meal Preparation	13
2.1.3 Detainee Meal Delivery	13
2.1.4 Detainee Menu Specifications	14
2.1.5 Detainee Meal Menu Requirements	14
2.1.6 Detainee Therapeutic Diets	15
2.1.7 Detainee Religious Diets	16
2.1.8 Detainee Holiday Menus	16
2.2. CSD Meal Service	17
2.2.1 CSD Daily Delivery.....	17
2.2.2 CSD Monday and Wednesday Delivery	17
2.3. ODR Meal Service	18
2.4. Food Service Staffing Requirements.....	19
2.4.1 Management and Supervision	19
2.4.2 Non-Management Employees	20
2.4.3 Staffing Plan & Reporting	20
2.4.4 Food Service Staff Training	21
2.4.5 Detainee Workers – Central Kitchen Location Only.....	21
2.4.6 Uniforms and Protective Clothing	22
2.5. Key Personnel.....	22
2.6. Food Service Contingency Plan	23
2.7. Facilities and Equipment	23
2.7.1 Facilities	23
2.7.2 Facilities Maintenance and Repairs	23

2.7.3	Food Service Equipment	24
2.7.4	Food Service Equipment Maintenance and Repairs	25
2.7.5	Supplies, Small Wares, and Commodities.....	25
2.8.	Sanitation and Pest Control	26
2.8.1	Sanitation.....	26
2.8.2	Pest Control Services.....	26
2.9.	Cost Accounting System & Reporting	26
2.9.1	Technology Requirements.....	28
2.9.2	Meal Services Reporting Requirements	29
2.10.	Quality Assurance & Control Plan	31
2.10.1	Quality Assurance Plan	31
2.10.2	Meal Quality Assurance	31
2.10.3	Inspection of Services.....	31
2.11.	Environmental Sustainability	32
2.11.1	Environmental Sustainability Plan	32
2.11.2	Recycling and Waste Management	32
2.12.	Good Food Purchasing Program.....	33
2.12.1	Good Food Purchasing Implementation Plan	33
2.13.	Non-Compliance.....	35
3.	<i>Current State</i>	35
4.	<i>Future State</i>	36
5.	<i>Proposed Solution</i>	36
5.1.	Solution Overview.....	36
5.2.	Software Overview	37
5.3.	Hosting and Platform Architecture Overview	37
5.4.	Integration/Interface	38
6.	<i>Solution Requirements</i>	38
6.1.	Hardware and Equipment Requirements	38
6.2.	Physical Environment Requirements.....	38
6.3.	Network Requirements	39
7.	<i>Implementation, Development and Project Management Services</i>	39
7.1.	Overview of the Implementation Methodology	39

7.2.	Project Task List and Timeline.....	40
7.3.	Assessment, Change Management and Reengineering Approach.....	40
7.4.	Requirements Validation and System Design/Configuration.....	40
7.5.	System Implementation and Configuration	41
7.6.	Data Conversion and Migration	42
7.7.	Quality Assurance (“QA”).....	42
7.8.	Knowledge Transfer /Training and Transition (Cutover).....	43
7.9.	Contract Performance Review and Acceptance	44
8.	<i>Solution Ownership and Other Terms and Conditions.....</i>	44
8.1.	Data Ownership	44
8.2.	Intellectual Property Ownership	45
8.3.	Hardware and Software Licensing	45
8.4.	Software and Hardware Warranties.....	45
8.5.	Other Terms and Conditions.....	46
9.	<i>Solution Performance and Availability</i>	46
9.1.	Hosting Services	46
9.2.	Support and Maintenance Service	47
9.3.	Data Access and Retention	47
9.4.	Business Continuity and Disaster Recovery.....	48
9.5.	Transition Out and Exit Requirements	49
9.6.	Transition of Commencement of Contract	50
9.7.	Continuity of Service.....	50
10.	<i>Security and Compliance.....</i>	50
10.1.	CCDOC Security Terms and Conditions.....	50
10.2.	Criminal Background Check	51
10.3.	Key Control	51
10.4.	Delivery to the CCDOC	51
10.5.	Data Security Controls.....	52
10.6.	Secure Development and Configuration Practices	52
10.7.	Compliance Requirements.....	53
10.8.	Incident Response Requirements.....	53
10.9.	Audit Requirements.....	54

11. Instructions to Proposers.....	54
11.1. Instructions	54
11.2. Availability of Documents.....	54
11.3. Pre-Proposal Conference	55
11.4. Mandatory Site Visit.....	55
11.5. Clarifications	55
11.6. Delivery of Proposal Package.....	55
11.7. Uniformity	55
11.8. Proposal Material.....	56
11.9. Addenda.....	56
11.10. Proposer’s Responsibility for Services Proposed	56
11.11. Errors and Omissions.....	56
11.12. RFP Interpretation	56
11.13. Confidentiality and Response Cost and Ownership	57
11.14. Use of Subcontractors.....	57
11.15. MBE/WBE Participation Goals.....	57
11.16. Proposer’s Disclosure and Conflict of Interest.....	57
11.17. Cook County RFP Format	57
11.18. Pricing.....	57
11.19. Period of Firm Proposal.....	58
11.20. Awards.....	58
11.21. Cook County Rights	58
11.22. Alteration/Modification of Original Documents	58
11.23. Recycling.....	58
12. Evaluation and Selection Process	58
12.1. Responsiveness Review.....	58
12.2. Acceptance of Proposals.....	59
12.3. Evaluation Process.....	59
12.4. Selection Process	59
13. Evaluation Criteria	60
13.1. Responsiveness of Proposal.....	60
13.2. Technical Proposal	60

14. Submission of Proposal.....	61
14.1. Instructions for Submission	61
14.2. Submission Requirements	62
Appendix I – Pricing Instructions	65
1. Items Included in Cost Per Meal	65
2. Optional Items Included in Cost Per Meal	65
3. Items Excluded from Cost Per Meal.....	65
4. Annual Price Adjustment.....	66
5. Payment	66
6. Optional non-CCDOC Mandated Meal Service (Meal Selection and Pricing)	67
7. Commission Return for Optional non-CCDOC Mandated Meal Service	67
8. Additional Pricing Terms and Conditions	68
Appendix II – Pricing Templates	69
Appendix III – Instructions for Submitting an Electronic Bid/Proposal/Qualification	69
Appendix IV – CCDOC Site Visit Security Procedure	72
Appendix V – General Meal Patterns	73
Appendix VI – Current Inventory of CCSO-Owned Equipment.....	74
Appendix VII – Cook County Good Food Purchasing Policy	80
Appendix VIII – Good Food Purchasing Standards and Scoring System.....	81
Appendix IX– CCDOC Non-Employee Credential Procedure	82
Appendix X – Economic Disclosure Forms	83
Appendix XI – Cook County Contract Agreement.....	84
Appendix XII – Addendum Acknowledgement Form	85
Appendix XIII – MBE/WBE Utilization Plan Forms	86
Appendix XIV – Identification of Subcontractor/Supplier/Subconsultant Form	87
Appendix XV – IT Special Terms and Conditions	88
1. Definitions for Special Conditions	88
2. Services and Deliverables.....	93
3. Warranties.....	95
4. Intellectual Property	97
5. Using Agency Data and Confidentiality.....	98
6. Data Security and Privacy	100

7. Data Security Breach 102

8. Audit Rights..... 103

9. Right to Exit Assistance 103

10. Miscellaneous 106

Appendix XVI – Computer Justice Information Systems [CJIS] Policy 108

Appendix XVII – System Matrix 108

1. Introduction

The Cook County Sheriff's Office ("CCSO") is soliciting Proposals from qualified Food Service Management Proposers to provide a full range of food services for the Cook County Department of Corrections ("CCDOC"). The objective of this Request for Proposal ("RFP") is to contract with a qualified Proposer that can provide a high-quality Food Service Management System, as outlined in this RFP, in a cost-effective manner. The Proposer shall provide services including, but not limited to staffing resources, training, products, specialty equipment, hardware, and software necessary to provide a quality Food Service Management system and meet the requirements outlined in this RFP.

The contract resulting from this RFP is expected to be three (3) years, with three (3), one (1) year options to renew. All terms and conditions of the original contract will apply throughout any renewal and extension periods.

1.1. Background

Cook County ("County") is an urban county in the upper northeastern section of the State of Illinois that contains more than 800 local governmental units within its boundaries. With a population of approximately 5.2 million people, it is the second most populous county in the nation and the 19th largest government in the United States (2010 census statistics).

It is a home rule county pursuant to Article VII, Section 6 of the Illinois State Constitution and is governed by a 17-member Board of Commissioners who are elected from single-member districts. The Commissioners and a County Board President are elected to four-year terms by the citizens of the County.

Cook County contains 132 municipalities in its region, the most well-known being the City of Chicago - which is the County seat where the central offices of Cook County are located. The City of Chicago and the suburban municipalities account for approximately 85% of the County's 946 square miles, while unincorporated areas make up the remaining 15%. The unincorporated areas of the County are under the jurisdiction of the Cook County Board of Commissioners.

As mandated by State law, County government has principal responsibility for the protection of persons and property, the provision for public health services and the maintenance of County highways. The CCSO operates the CCDOC, one of the largest single-site county facilities in the United States which is comprised of multiple Divisions segregated by security and programming classifications. Primarily holding pre-trial detainees, the CCDOC admits approximately 100,000 detainees annually, with an average daily custodial population of approximately 8,000, which includes electronic monitoring. The facility covers more than eight city blocks and each Division has a unique layout that includes, but is not limited to, a visiting area, dispensary, law library, multi-purpose room, detainee classrooms, living units with dayroom and staff offices.

1.2. Business Goals and Objectives

The CCSO objectives for the Food Service Management System are to:

- A. Provide meals and food service to detainees and staff, seven (7) days a week, at an estimated quantity of 7,110,894 meals per year, in compliance with all Food Safety Regulatory Authorities, local, county, state, federal laws and regulations relating to standards for food service in correctional facilities, including but not limited to, the Illinois Jail Standards Act, the Illinois Administrative Code Title 20, Chapter I, Part 701, the Illinois Food Handling Regulation

Enforcement Act (410 ILCS 625), and Illinois Department of Public Health Food Service Sanitation Code (77 Ill. Adm. Code 750).

B. Provide the following related technology services:

1. A food service management cost accounting system to account for all detainee meals served over the course of the contract as is set forth in Section 2.9. This system, which must include all necessary technology, equipment, and any other essential resources, must have the ability to integrate and/or interface with the CCDOC Jail Management System in order to establish an efficient and reliable automated meal ordering system that provides computerized meal ordering, billing, and inventory. Proposer shall implement and maintain this system over the course of the contract.

The CCDOC Jail Management System is a Microsoft Dynamics 365-based system architected and implemented by DXC Technologies. The fields required for integration/interfacing with the Jail Management System are identified in section 2.9 B, and 2.9.1 below.

2. An automated process to account for all Staff Meals served over the course of the contract as is set forth in Section 2.9. This system, which must include all necessary technology, equipment, and any other essential resources, must be utilized as the billing system for all ODR locations. Proposer shall implement and maintain this system over the course of the contract.

- C. Establish a Food Handler's Certification Training program for detainees that supports the CCSO's mission of offering training to detainees that equips them with a skill set and decreases the likelihood of recidivism. Proposer must submit a training manual to address the training procedure and methodology.

1.3. Schedule

The following timetable establishes the projected dates and times of certain critical events relative to this RFP, including submission of written inquiries to the County, submission of Proposals and the consideration of Proposals by the Evaluation Committee. The County may revise or supplement this schedule via an Addendum.

The County anticipates the following Schedule:

RFP Posted to the website	Friday, December 4, 2020
Proposer Registration Deadline for Mandatory Site Visit	Thursday, December 10, 2020 by 12:00pm (noon)
Pre-Proposal Conference	Tuesday, December 15, 2020 12:00pm (noon)
Mandatory Site Visit ¹	Wednesday, December 16, 2020 Times will be scheduled for each vendor
Proposer Inquiry Deadline	Wednesday, December 23, 2020 by 12:00pm (noon)
Response to Inquiries	Wednesday, December 30, 2020
Proposal Due Date	Wednesday, January 13, 2021 by 10am

¹ Proposer shall only be permitted to conduct a Site Visit after completing the CCDOC Site Visit Procedure set forth in Appendix IV.

1.4. Definitions

Whenever used in the RFP, attachments, or addendums the following terms will have the meanings defined below. Any questions regarding these definitions should be addressed to the Chief Procurement Officer as identified in this RFP.

- A. “*Executive Director/designee*” shall mean the Executive Director of the Cook County Department of Corrections, or persons identified to Proposer by the Executive Director as being authorized to act for or on behalf of the Executive Director.
- B. “*CCDOC*” shall mean the Cook County Department of Corrections. CCDOC and CCSO may be used interchangeably to refer to the management and oversight of operations within CCDOC facilities.
- C. “*CCDOC Central Kitchen*” or “*Central Kitchen*” shall mean the location within CCDOC that serves as the primary kitchen in which meals for CCDOC detainees are prepared.
- D. “*ODR*” shall mean the Officer’s Dining Room. Currently, the ODR is located in Division 5 on the CCDOC jail compound. However, the number and location of ODR’s is subject to change based on the operational needs of the CCSO.
- E. “*CCHHS*” shall mean the Cook County Health and Hospital Systems; Cermak Hospital operates within CCDOC and provides medical services to detainees, under the umbrella and directions of CCHHS.
- F. “*CSD*” shall mean the Court Services Department.
- G. “*Food Service Management System*” shall mean the provision of food services to all detainees, staff and designated visitors for meals that are provided by the Proposer to CCDOC and CSD Lock-Ups and approved by the CCSO.
- H. “*Integrated/Integration*” refers to two or more components merged into a single system sharing a single set of data. For example: Increasingly, the term integrated software is reserved for applications that combine word processing, database management, spreadsheet functions, and communications into a single package.
- I. “*Interface*” shall mean boundary across which two independent systems meet and act upon or communicate with each other.
- J. “*Acceptance*” means the acceptance of the successful Implementation of the complete “System” and successful completion and delivery of all Deliverables as set forth herein.
- K. “*Application*” means the software(s) proposed to fulfill the County’s requirements under this RFP, regardless of whether the proposer has manufactured or created the software(s).

- L. “*Cloud Computing*”² or “*Cloud*” means a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
- M. “*Hosting*” means the environment in which the Application and corresponding services (e.g., SaaS, PaaS, or IaaS) are deployed, regardless of whether such environment is On-Premises, Remotely Hosted, or in the Cloud, and regardless of whether a party other than the proposer provides such environment and services. Hosting is included within the definition of System.
- N. “*Hybrid Cloud*” means a Cloud infrastructure composed of two or more distinct Cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).
- O. “*Hybrid Hosting*” means a combination of two or more of the following: On-Premise Hosting, Remote Hosting and/or Cloud Computing. Hybrid Hosting is different than Hybrid Cloud.
- P. “*Infrastructure as a Service*” or “*IaaS*” means a service model where the provider provisions processing, storage, networks, and other fundamental computing resources to the County for deploying and running arbitrary software, where the County does not manage or control the underlying infrastructure but where the County has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).
- Q. “*Platform as a Service*” or “*PaaS*” means a service model where the County deploys its own applications onto the provider’s infrastructure using provider-supported coding languages and tools, but where the County does not manage or control the underlying infrastructure.
- R. “*Software as a Service*” or “*SaaS*” means a service model where, via a web browser or other interface, the County is to use the provider’s applications running on a Cloud Computing infrastructure, but where the County does not manage or control the underlying infrastructure.
- S. “*System*” means the Application, other software, hardware, processes, services and Hosting proposed to fulfill the County’s requirements under this RFP, regardless of whether the aforementioned are County-specific customizations or the proposer’s standard offerings.
- T. “*Integrated/Integration*” refers to two or more components merged together into a single system sharing a single set of data. For example: Increasingly, the term integrated software is reserved for applications that combine word processing, database management, spreadsheet functions, and communications into a single package.
- U. “*Interface*” shall mean boundary across which two independent systems meet and act upon or communicate with each other.

² Cook County generally follows the definitions of the National Institute of Standards and Technology (“NIST”) relating to cloud computing, which this RFP loosely summarizes. Proposers should find the complete NIST definitions set forth in NIST Special Publication 800-45, available at: <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf> (last visited December 18, 2019).

- V. “*Jail Management System/JMS*” assists with the full management of a jail or correctional facility, including booking, pre-booking, tracking detainee movement, classification, discipline, prisoner funds, court services, and facility data including inventory.
- W. “*Proposer*” shall be meant to refer to the Food Service Management System Proposer responding to this Request for Proposal. The Proposer has sole responsibility for providing the proposed solution, and related support services.

2. Scope

Proposer’s food service deliverables under this RFP shall generally fall into three main categories:

- A. Meal service to the CCDOC detainee population housed within Cook County Jail (hereinafter “Detainee Meal Service”)
- B. Meal service to CSD Lock-up (hereinafter “CSD Meal Service”)
- C. Meal service to CCSO staff and authorized visitors in designated ODR location(s) (hereinafter “ODR Meal Service”)

The specifications for each of these categories shall be addressed in the following sections. The general conditions throughout this RFP are intended to apply to each and all Food Service categories described in these sections.

2.1. Detainee Meal Service

2.1.1 Detainee Meal Orders

The meal orders shall be generated electronically for all three (3) meals, via software provided by the Proposer, containing the total number of detainee meals to be served for the applicable meal—breakfast, lunch, or dinner—and the total number of each and any therapeutic diet meals to be served within those totals.

Currently, the CCSO submits completed meal order forms to the food service provider, three (3) times per day, containing the total number of detainee meals to be served for the applicable meal—breakfast, lunch, or dinner—and the number of each and any therapeutic/specialty diet meals to be served within those totals. The meal orders are submitted at least one (1) hour prior to the scheduled meal delivery time. Listed below are times in which the current orders are placed:

- Lunch: 8:00 a.m. CST
- Dinner: 3:00 p.m. CST
- Breakfast: 3:00 p.m. CST previous working day

The Proposer shall provide a computerized daily meal order report that shall include, but not be limited, to the following information:

- A. Date and time meal order was placed
- B. Type of meals ordered

- C. Number of meals ordered
- D. Number of meals changed
- E. Number of meals served
- F. Number of meals returned
- G. Location for which the meals were ordered.

2.1.2 Detainee Meal Preparation

Proposer shall prepare all detainee meals on-site in the CCDOC Central Kitchen. Proposer may rely on off-site prepared meals only in the event of an emergency and/or if the CCDOC Central Kitchen is unavailable, and shall obtain approval from the CCSO prior to preparing any meals off-site. In no case shall the Proposer serve meals which fail to conform to the specified guidelines and standards for food quality and preparation set forth herein.

2.1.3 Detainee Meal Delivery

The CCSO shall establish a food service delivery schedule that corresponds with detainee breakfast, lunch, and dinner meal service. The CCSO's current delivery schedule is as follows, subject to change based on reasonable notice to the Proposer:

- Lunch: 11:00 a.m. CST
- Dinner: 4:00 p.m. CST
- Breakfast is delivered the previous workday with the Dinner meals to accommodate court schedules.

Reliable and timely delivery of meals to CCDOC delivery locations at a reasonable interval for breakfast, lunch, and dinner is essential to meet detainee daily diet needs and maintain compliance with food safety standards. Per the Illinois Jail Standards, no more than 14 hours shall be maintained between the evening meal and the next morning breakfast. Proposer must describe in their Proposal how they will maintain compliance with the following minimum requirements:

- A. Proposer shall place prepared meals into insulated food carts provided by the CCSO, loaded to maximize efficient transportation and distribution of meals, according to the CCSO's food service delivery schedule.
- B. Proposer shall position the loaded food carts in the CCDOC designated area within Central Kitchen. The CCSO will pick up food carts from the designated area and deliver to all delivery locations.
- C. The Proposer shall package breakfast and lunch meals in a single, sealed, transparent containers that protect food products from contamination by insects or foreign substances.
- D. Proposer shall utilize insulated compartmented trays provided by the CCSO for dinner meals. It may be necessary for Proposer to provide and utilize single use packaging as directed by the CCSO.

2.1.4 Detainee Menu Specifications

Meal patterns that have been traditionally utilized by the CCSO are set forth in Appendix V. Proposers shall include proposed menus in their proposal based on the examples provided in Appendix V and the additional specifications contained herein. Upon award of the contract, the selected Proposer shall strictly provide all items on the approved food service menu. Menu substitutions must be submitted to the CCSO for approval at least twenty-four (24) hours in advance. All menu substitutions shall be tracked and maintained for a minimum duration of ninety (90) days and must be provided upon request by regulatory authorities in the event of epidemiological investigation during foodborne illness incident or any other food safety related issues.

All detainee menu items must be reviewed and approved by the CCSO to ensure compliance with security protocols and policies.

2.1.5 Detainee Meal Menu Requirements

Detainee Meals are strictly regulated to ensure compliance with Illinois Jail Standards, as well as related policies and procedures. Proposer must provide healthy and nutritious meals with a total daily caloric intake of 2,300-2,500 calories that are low fat, low sodium and appropriate for CCDOC's detainee population.

The Proposer shall meet the following requirements for all detainee meals:

- A. No pork product or pork derivative may be on the menu.
- B. No seafood product or seafood derivative may be on the menu.
- C. The same type of meat shall not be served more than once a week.
- D. No alcohol or alcohol derivative may be used in the preparation of meals on the menu.
- E. Milk shall be served a minimum of one (1) time per day in individual 8-ounce portions.
- F. In addition, a minimum 10% fruit juice drink shall be served with the breakfast meal, fortified with Vitamin C, supplied in individual 4-ounce portions. A fruit drink (8 ounces) shall be served with the lunch meal.
- G. Jelly shall be provided at all breakfast meals except when syrup is required.
- H. Wheat bread must be served two meals per day; the third meal may be white bread.
- I. When donuts, dinner rolls, buns or cornbread appears on the menu additional bread is not required for the meal. Donuts, if not the cake type, must be iced. Plain pastry shells which are meant to contain filling shall not be used.
- J. The same type of dessert may be served within a one (1) week period, but not on consecutive days. The names of desserts scheduled to be served must appear on the menus; the word "dessert" alone is unacceptable.
- K. Potato or macaroni salad may be used as a starch, as long as another salad type item is served; at no time will an increase in these salad quantities be allowed to count as both the starch and salad

requirement. A minimum of two (2) types of salad dressings must be served (i.e. Italian, French, etc.) but not on consecutive days.

L. Fruit options may be restricted at CCSO's direction based on considerations related to institutional safety.

M. Red pepper bologna is prohibited from use by the Proposer.

Examples of proposed menus shall be submitted with the proposal. Proposed menus shall include the following nutritional information for all detainee meals:

- Calories (kcal)
- Fat (gm)
- Percent of calories from fat (%)
- Saturated Fat (gm)
- Percent of calories from saturated fat (%)
- Protein (gm)
- Carbohydrate (gm)
- Cholesterol (mg)
- Sodium (mg)

The Proposer shall not use food that has been prepared or stored in violation of any applicable Food Safety code, or regulation including Federal, State and Local Food Safety Regulations.

2.1.6 Detainee Therapeutic Diets

The Proposer shall prepare and deliver therapeutic diet meals where such diets are ordered by Cook County Health and Hospitals System ("CCHHS") personnel. Therapeutic diets shall conform to all dictated medical criteria and shall be served as ordered. The CCSO anticipates that Proposer shall serve approximately 61,230 therapeutic meals per month, which may be subject to fluctuation as a result of external conditions beyond the control of the CCSO.

The Proposer shall provide healthy snacks, juices, milk and all other items included in the prescribed medical diets identified in this section; as prescribed medical diets may be amended from time to time, such changes shall be included in the cost of the meal and shall not be billed separately by Proposer.

The Proposer shall submit a copy of its dietary manual and provide examples of dietary menus with their proposal submission to demonstrate Proposer's experience with, and knowledge of, therapeutic diets and adapting meals based on medical restrictions. Proposed therapeutic diet menus shall include the nutritional information required in Section 2.1.5. The following is a listing of the current therapeutic diets, all of which shall be made available daily, upon request:

- A. Cholesterol/Fat Restricted/Low Salt (300 mg cholesterol, 30% Fat, 4gm NA)
- B. Dental Soft
- C. Nutrition Support Diet with Healthy Snack
- D. Diabetic 2400 Cal A.D.A. with Healthy Snack

- E. 3200 Cal A.D.A. with Healthy Snack
- F. Pregnancy with Healthy Snack
- G. Full Liquid
- H. Clear Liquid Diet
- I. Renal Diet
- J. Vegan
- K. Food Allergy/Other Diets (i.e. No Lactose, No Gluten, No Peanut, etc.)

The vast majority of the therapeutic diet meals served are the low cholesterol, low-fat diet. Notwithstanding, this list is not exhaustive, and Proposer is expected to make any modified therapeutic dietary meal available at the direction of CCSO and CCHHS. Each therapeutic diet carries restrictions and requirements to be followed in accordance with the Illinois Jail Standards and based on CCHHS direction.

Food Allergy/Other Diets labeled No-Pork or No-Seafood shall be considered a Regular Diet meal and not a Therapeutic Diet meal.

2.1.7 Detainee Religious Diets

Proposer shall provide meals for detainees in accordance with the Religious Land Use and Institutionalized Persons Act (RLUIPA), 42 U.S.C. §§ 2000cc, et seq., and comply with all other federal, state, or local laws and court decisions. Compliance with the RLUIPA shall not result in any additional fees or charges to the CCDOC.

The CCSO shall be responsible for processing all written detainee requests for religious meals by way of CCDOC Inmate Services or designee, in accordance with applicable CCSO policies and procedures. All approved detainee requests shall be forwarded by CCSO to the Proposer for implementation.

The Proposer must provide certified meals for religious diets as described in Religious Diet Programs, Certified Food Components, Ch. 4-1, Food Service Manual published by the U.S. Bureau of Prisons (2011) or most recent edition.

Examples of proposed religious diet menus shall be submitted with the proposal. Proposed religious diet menus shall include the nutritional information required in Section 2.1.5.

2.1.8 Detainee Holiday Menus

Proposer shall prepare holiday menus for meals to be served on the following holidays: New Year's Day, July 4th, Thanksgiving and Christmas. The Proposer shall also prepare holiday menus on Easter, Memorial Day, and Labor Day or in the alternative provide one (1) monthly Saturday or Sunday Dinner Meal that includes a whole meal meat (e.g., Fried Chicken, Roast Beef or Turkey-Ham), for each month that does not include a mandatory Holiday Menu. All menus provided under this section shall be submitted at least one (1) month in advance for approval by the CCSO. The cost for Holiday meals shall be the same cost per meal as a regular diet meal.

The Proposer shall adjust the therapeutic diet meals to reflect the aforementioned holidays where feasible. Portions provided shall equal or exceed those provided by non-holiday menus.

Examples of proposed holiday menus shall be submitted with the proposal. Proposed holiday menus shall include the nutritional information required in Section 2.1.5.

2.2. CSD Meal Service

The CCSO anticipates that the Proposer shall serve approximately 135,952 CSD meals per year, which may be subject to fluctuation as a result of external conditions beyond the control of the CCDOC. CSD meals differ from the CCDOC detainee meal requirements as well as delivery requirements set forth herein. All CSD meals shall consist of the following:

- A. Two (2) sandwiches – each sandwich shall contain:
 - two (2) slices of bread; and
 - three (3) ounces of meat; OR two (2) ounces of meat and two (2) ounces of cheese
- B. Two (2) condiment packets; and
- C. One (1) eight (8) ounce fruit drink.

2.2.1 CSD Daily Delivery

The Proposer shall provide a meal for each detainee in CSD Criminal Courts Building lock-up, one (1) time per day, seven (7) days per week.

- Criminal Courts Building – 2600 S. California Ave., Chicago Illinois 60608

CCSO shall provide the Proposer with the requested CSD meal order count daily for the Criminal Courts building. The Proposer shall prepare the CSD meals, and place the requested quantity in the CCDOC designated area within Central Kitchen. CCDOC will deliver the meals to the CSD Criminal Courts lock-up according to the following delivery schedule, subject to change based on reasonable notice to the Proposer:

- Monday through Friday: 10:00 a.m. CST; and
- Saturday, Sunday, and Holidays: 7:00 a.m. CST

2.2.2 CSD Monday and Wednesday Delivery

The Proposer shall provide a meal for each detainee at the following CSD courthouses one (1) time per day on Monday and Wednesday.

- Domestic Violence Courthouse – 555 W. Harrison Street, Chicago Illinois, 60607
- Police Courts North – 5555 W. Grand Avenue, Chicago Illinois, 60639
- Police Courts North – 3150 W. Flournoy, Chicago Illinois 60612
- Police Courts South – 727 E 111th Street, Chicago, Illinois 60628
- Richard J. Daley Center Courthouse – 50 W. Washington Street, Chicago, Illinois 60602
- Skokie Courthouse – 5600 W. Old Orchard Rd., Skokie, Illinois 60076
- Maywood Courthouse – 1401 S. Maybrook Drive, Maywood, Illinois 60153

- Markham Courthouse – 16051 S. Kedzie Parkway, Markham Illinois 60428
- Bridgeview Courthouse – 102220 S. 76th Avenue, Bridgeview, Illinois 60453
- Rolling Meadows Courthouse – 2121 Euclid Avenue, Rolling Meadows, Illinois 60008

CCSO shall provide the Proposer with a schedule of the Monday and Wednesday meal order count for each CSD courthouse listed above. The Proposer shall prepare the CSD meals, and deliver the total quantity specified for each day to the CCDOC designated area within Central Kitchen on Monday and Wednesday, respectively. CCDOC will deliver the meals every Monday and Wednesday to the above CSD courthouses at 10:00 a.m. CST. The meal order count and the time meals are delivered to the CSD courthouses by CCDOC are subject to change based on reasonable notice to the Proposer.

2.3. ODR Meal Service

The Proposer shall provide food services for CCSO staff and authorized visitors in all designated Officer Dining Rooms (“ODR”). The CCSO anticipates that Proposer shall serve approximately 65,940 ODR meals per year.

Currently, there is one (1) ODR on the CCDOC compound located in Division 5. However, the number and location of Officer Dining Rooms is subject to change based on the operational needs of the CCSO. The ODR shall be open 24/7 to accommodate all shifts, any modification to this schedule must be approved by the CCSO.

The Proposer shall meet the following minimum requirements for ODR meals:

- A. One (1) hot entrée. Entrees must contain at least 3 oz. of meat; one entrée item must be a whole meat. Portion size: 1 serving. Meat patties and casseroles shall be served no more than two (2) times per week.
- B. Two (2) types of sandwiches. Each sandwich must contain at least three (3) ounces of meat, fish or poultry.
- C. One (1) type of grill item, such as hot dogs (jumbo only), polish sausage, hamburger, grilled cheese, etc. Portion size: 2 grilled cheese, all others one item.
- D. Made to Order Salads. The following items are required, at all times for Made-to-Order salads: Pasta Salad, Coleslaw, Plain Tuna, Mixed Salad Greens, Fresh Spinach, Tomatoes, Broccoli, Green Peppers, Cauliflower, Onions, Carrots, Cucumbers, Cheese, Croutons, and four (4) types of Salad Dressing.
- E. A pre-packaged nutrient-dense salad is allowed in addition to the made to order salads, with a choice of at least four (4) types of salad dressing.
- F. One (1) starch item, such as potatoes, rice, and/or noodles. Portion size: 1 cup.
- G. One (1) vegetable item, such as California blend, oriental blend, broccoli, and/or greens. Portion size: ½ cup.
- H. One (1) dessert item, such as fresh fruit, cake, cobblers, ice cream, and/or pie. Portion size: one (1) each.

- I. Two (2) types of bread, such as wheat, white, rye, and/or pumpernickel. Portion size: two (2) slices.
- J. Self-serve Beverages, including all of the following: Coffee, tea, milk, fruit drink, assorted soft drinks and water.
- K. Self-serve condiments, such as salt, pepper, ketchup, mustard, mayonnaise, relish and hot sauce.

Examples of proposed ODR menus shall be included in the proposal submission.

Upon award, contracted Proposer shall post menu plans in the ODR at least one week in advance. Menu revisions shall be submitted to the CCSO for approval at least two (2) weeks before planned implementation. Menu substitution must be submitted for approval at least twenty-four (24) hours in advance. All menu substitutions shall be tracked and maintained for a minimum duration of ninety (90) days and must be provided upon request by regulatory authorities in an event of epidemiological investigation during foodborne illness incident or any other food safety related issues.

2.4. Food Service Staffing Requirements

As required by the Illinois Department of Public Health Food Service Sanitation Code (77 Ill. Adm. Code 750), any person working with or around food shall be trained in food safety and sanitation and shall possess and maintain a Food Handler Certification. The current staffing level in both Central Kitchen and ODR is approximately 63 employees. Of these, eight (8) in Central Kitchen and two (2) in ODR are management staff.

The Proposer shall provide qualified civilian staff at the CCDOC Central Kitchen and ODR locations. Proposer's staff, in conjunction with assigned detainee workers shall prepare all detainee and CSD meals in the CCDOC Central Kitchen.

Detainees are strictly prohibited from preparing any food to be served in conjunction with ODR meals.

The Proposer shall describe the level of support and supervision required during the food service preparation process. Level of support and supervision such as detainee workers and security supervision may be subject to fluctuation as a result of external conditions beyond the control of the CCSO.

The Proposer shall describe the hiring practices and training procedures for employees assigned to service this contract. Proposer training must be documented, and the records made available for review by the CCSO and Cook County upon request. The Proposer shall require its on-site employees to complete any and all applicable CCSO civilian training or orientation prior to work assignment.

2.4.1 Management and Supervision

The Proposer shall provide direct supervision to ensure regulatory food safety and sanitation standards are met, and equipment is utilized according to manufacturer specifications.

The Proposer shall provide adequate supervision of all food service staff, including detainee workers, at all times and in all areas of food service operation. These include a sufficient number of Managers with Food Safety and Sanitation Manager Certifications (FSSMC) or Food Handlers to supervise each post. The supervisory staff positions set forth in this Section shall be in attendance whenever the facilities are in operation and shall be assigned exclusively to the performance of Proposer's obligations under this contract

to assure quality performance. Any change in supervisory personnel must be cleared in advance and approved by the CCSO.

The Proposer shall include proposed operational policies and procedures (i.e. Sanitation, HACCP, training, tool security and inventory, etc.) that will be followed by its employees assigned to service this contract, with their proposal submission.

2.4.2 Non-Management Employees

The Proposer shall also provide a sufficient number of non-management employees to meet all requirements of this food service contract, including proper direct supervision of detainee workers. The current non-management staffing level in both Central Kitchen and ODR is approximately fifty-three (53) employees. Please note: the current staffing level for Central Kitchen is based on the current contract providing up to 250 inmate workers per 24-hour period. Proposer shall comply with the following minimum standards as it related to non-management employee staffing:

- A. CCDOC Central Kitchen Food Line: One (1) Proposer non-management employee shall be assigned to monitor each food line in the CCDOC Central Kitchen while in operation.
- B. CCDOC Central Kitchen Sandwich Production: At least two (2) Proposer non-management employees shall be assigned to supervise sandwich production.
- C. CCDOC Central Kitchen Tray Wash Area: No less than two (2) Proposer non-management employees shall be present to supervise tray washing operations.
- D. CCDOC ODR Locations: Proposer shall ensure all ODR non-management employees possess valid food handler certification within thirty (30) days upon employment and subsequently renew thereafter according to the expiration date. ODR must be operational 24 hours per day, 7 days per week. No detainee workers shall be assigned to work in ODR locations.

2.4.3 Staffing Plan & Reporting

Proposer shall provide a complete staffing plan with their proposal, which includes: the total number of management staff, and non-management staff by location; a daily staff (managers and employees) assignment schedule for each shift and work group (based on regular days off); an organizational chart; and job descriptions for all positions.

Upon award, the contracted Proposer shall:

- A. Keep a complete roster of all employees assigned to perform services under the contract, that includes both filled positions with staff names and start date and vacant positions with date vacated, and provide a current, electronic copy of same to the CCSO monthly.
- B. Provide timesheets for all employees, including managers, for each shift, work group and work location to the CCSO within 48 (forty-eight) hours after the close of each pay period for the duration of the contract.
- C. Maintain standard operating procedures governing the daily assignment of the work within Food Management Services under the contract. Delegation of authority within Food Management Services will be clearly defined in the standard operating procedures for the duration of the contract.

- D. Comply with all CCSO policies, procedures and directives relevant to food service operations and shall communicate these policies, procedures and directives to all Proposer employees assigned to this contract.
- E. Maintain Food Safety and Sanitation Manager and Food Handler Certificates for employees assigned to perform services under the contract. Certificates shall be provided upon request from CCSO and all Regulatory Authorities.

2.4.4 Food Service Staff Training

Proposer's employees are required to attend applicable civilian training and/or orientation provided by the CCSO. New Proposer employees must attend forty (40) hours of orientation/training during the first six (6) months of assignment under the contract. The forty (40) hours of training will be the responsibility of the Proposer.

The Proposer will ensure that all Food Service staff has access to the Illinois Food Sanitation Code and the U.S. Public Health Service Food Code. Proposer shall also provide annual training for its employees servicing the contract that incorporates relevant CCSO policies and procedures and any specific training necessary for Proposer employees operating equipment that includes, but is not limited to: (i) proper operation, cleaning, and sanitizing of all equipment; (ii) the inherent dangers of each piece of equipment; (iii) symptoms of equipment malfunction; and (iv) staff responsibility to immediately report all hazards, malfunctioning equipment, or unsafe conditions to their supervisors.

All training must be documented, and the records made available for review by the CCSO and Cook County upon request.

2.4.5 Detainee Workers – Central Kitchen Location Only

Detainees are strictly prohibited from preparing food to be served in ODR, however Proposer shall utilize detainee workers to prepare Detainee Meals and CSD Meals. Proposer shall provide a description of all proposed detainee worker assignments and shift schedules with their proposal.

The CCSO will make available a pool of up to one hundred (100) detainee workers per 24-hour period. If more than one hundred detainees are required by the Proposer, the Proposer will compensate the County, for the additional detainees, based upon current detainee payroll rates in effect at the time of the request. The current detainee payroll rate is \$3.00 per shift of work for detainees with dishwashing assignments, and \$2.00 per shift of work for detainees with all other assignments.

Proposer shall be responsible for training all assigned detainee workers in the performance of their assigned tasks. Proposer shall collaborate with the CCSO in the design and implementation of a Kitchen Worker Orientation Training program. Said training shall include, at minimum, instruction as follows: Central Kitchen Security Rules & Regulations; Food preparation and handling procedures; Sanitation and proper grooming; Energy conservation methods; Recycling; Handling waste and properly recycling non-waste materials during the preparation and service of meals; and any other area the Proposer deems necessary for the performance of this contract.

Proposer must comply with the Illinois Food Handling Regulation Enforcement Act in utilizing detainee workers. *See* 410 ILCS 625. Proposer shall ensure that all detainee workers acquire food handling certifications during the course of each detainee worker's food service assignment at no cost to the CCSO or County.

2.4.6 Uniforms and Protective Clothing

Proposer shall submit a detailed description of the uniforms proposed to be worn by on-site Proposer employees. Employee uniforms shall be black or white in color. All Proposer employee uniform costs shall be borne by the Proposer.

The CCSO shall provide food service detainee worker uniforms, which shall consist of a red and white striped one-piece jumpsuit/coverall with "Cook County Department of Corrections" silk screened in black color on the uniform back. The Proposer shall provide laundry services for detainee uniforms to ensure clean uniforms on a daily basis for detainee workers.

The Proposer shall provide detainee workers with hair net/hats, beard guards, plastic/cloth aprons, plastic gloves, rubber gloves and rubber boots for tray washing. No employee or detainee uniforms or other items listed in this section may be considered part of the Cost per Meal.

2.5. Key Personnel

The Proposer shall submit a current organizational chart of its key positions including, but not limited to, executive and management staff with names and titles. Qualifications of Key Personnel shall be submitted with Proposer's response to this solicitation, including resumes reflecting certifications and experience working within food service systems for institutions of similar scale to CCDOC, if applicable. Specific qualification requirements for Key Personnel are detailed in this Section.

- A. Food Service Director: Proposer shall specifically provide a Food Service Director dedicated solely to this contract. The Food Service Director shall have at least three (3) years of experience in the field of large institutional food service management. Upon award, the contracted Proposer shall not remove or reassign the Food Service Director from the CCDOC for a minimum period of one (1) year without the approval of the CCSO, unless removal is requested by the CCSO.
- B. Food Service Managers: Proposer shall ensure that at least one (1) Food Service Manager is on-site at all times during food preparation, per the Illinois Administrative Code. Food Service Managers shall have all requisite food service and public health certifications under federal, state, county and local law for food service operation. As food served in ODR must be prepared separately from food prepared for Detainee and CSD Meals, Proposer must ensure that a licensed Food Service Manager is present in each location during all food preparation.
- C. Registered Dietitian: The Proposer shall also provide at least one (1) full time, on-site Dietician registered and licensed by the State of Illinois. Proposer's Dietician shall not work in the capacity of the Food Service Director or Food Service Manager. The Proposer Dietician's responsibilities shall include, but not be limited to, the following:
 - 1. Manage the daily provision of therapeutic diets.
 - 2. Help resolve problems related to therapeutic diets.
 - 3. Monitor the Hazard Analysis and Critical Control Points ("HAACP") program, document related problems and solutions.
 - 4. Monitor Quality Assurance and Sanitation, document related problems and solutions.

5. Generate and approve regular and therapeutic menus for use at CCDOC.
6. Conduct in-service training for the Proposer's employees and for detainees who participate in the provision of services as detailed herein.
7. Work with the CCSO, as well as CCHHS/Cermak Health Services to resolve problems related to the food service operation.

2.6. Food Service Contingency Plan

The Proposer shall prepare and submit with the proposal a Contingency Plan for providing uninterrupted food services in the event of lockdowns, strikes by Proposer's employees, riots, fire, power failure or other catastrophic events that may curtail or impact the normal operations of the CCDOC. The Contingency Plan and any future amendments shall include, but not be limited to the following:

- A. A step by step outline of the Proposer's plan of action in the event of a catastrophic occurrence, listing (when appropriate) names, phone numbers and addresses of contacts.
- B. Designation of offsite locations that comply with local Department of Health and/or Federal Food Safety Codes for food preparation and storage.
- C. Alternative staffing plans.
- D. Any other information Proposer deems necessary to demonstrate its capability to provide uninterrupted service in the event of a catastrophic occurrence.

2.7. Facilities and Equipment

2.7.1 Facilities

The CCSO shall provide the Proposer with access to the CCDOC Central Kitchen, ODR Kitchen, and storage facilities, including sanitary toilet and locker room facilities for use by food service employees. The Proposer shall use such facilities in the performance and delivery of food services.

The Proposer may, in furtherance of its obligations under the contract, utilize local Department of Health licensed preparation and storage facilities located outside the CCDOC on an emergency basis with the prior approval of the CCSO, pursuant to Proposer's Contingency Plan, as set out pursuant to Section 2.6. CCDOC facilities made available to the Proposer under the contract may not be used for any operations unrelated to the performance and delivery of food services under the contract.

2.7.2 Facilities Maintenance and Repairs

Cook County Facilities Management ("Facilities Management") shall be responsible for proper preventative maintenance and repair of the CCDOC building structure, including roof, ceilings, walls, floors, docks, exterior surfaces, plumbing and sewers behind floor or walls, elevators and general fire protection systems, electrical systems, security monitoring systems and all other structural components of the buildings.

The CCSO will be responsible for maintaining all drains in the kitchen areas. The Proposer is responsible for properly handling pre-cleaning of food trays, etc., to ensure the drains stay clean and free of debris. The Facilities Management shall be responsible for all other structural plumbing matters, unless the damage to plumbing systems is due to Proposer's neglect.

Repairs due to negligence or abuse by the Proposer's employees or detainee workers due to inadequate supervision or training will be charged to the Proposer. The Proposer shall define and document the need for building repairs by initiating a work order through the CCSO's established procedures. The point of contact for repairs will be designated by the CCSO.

2.7.3 Food Service Equipment

The CCSO shall provide the Proposer existing CCSO-owned food service equipment in the CCDOC Central Kitchen, ODR Kitchen, and all other designated locations for use by Proposer during the term of the contract. A current list of CCSO-owned food service equipment is included in Appendix VI. All such equipment shall remain the property of the CCSO.

- A. Upon award of the contract, Proposer and the CCSO shall jointly conduct an initial inventory of food service equipment provided by the CCSO. As part of this inventory an assessment of the condition and expected useful life of each item will be made. Unless otherwise expressly noted, it shall be presumed that the Proposer accepts the equipment as initially inventoried, as in good working order, and sufficient for the purpose of performing the contract.
 - 1. Following the initial inventory of equipment, Proposer and the CCSO shall conduct a joint inventory of equipment semi-annually, not later than June 30 and December 31 for each year of the contract.
 - 2. On a quarterly basis, the Proposer shall report on the status and condition of the equipment to the CCSO. Such report shall state with specificity the Proposer's recommendations for equipment maintenance and replacement.
- B. The Proposer shall be responsible for maintaining records of all equipment added, replaced and/or removed from the initial inventory that shall be made available to the CCSO upon request. Equipment records shall include sufficient information to document the following:
 - 1. Description of the equipment including the manufacturer's name, make and model of the equipment, manufacturer's identification number, useful life of the equipment, and the date the equipment was placed into service.
 - 2. The date(s) the equipment received preventative maintenance and the name of the company providing preventative maintenance.
 - 3. The date(s) the equipment was repaired due to malfunction or damage, a description of the malfunction or damage, and the name of the company providing repairs.
- C. If the Proposer deems necessary, Proposer may purchase additional equipment to aid in the increased efficiency and delivery of contract services. Equipment purchased or added by Proposer shall meet the National Sanitation Foundation (NSF) or Underwriters Laboratories (UL) standards. Equipment purchased by the Proposer must be added to the inventory and designated as "Proposer Owned" on all inventory reports. Said equipment shall remain the property and sole responsibility of the Proposer at the end of the contract term.
- D. At the end of the contract term, or upon termination of the contract, the Proposer and the CCSO shall jointly conduct a closing inventory, documenting additions and deletions from the initial inventory and evaluating the condition of all CCSO-owned equipment. The Proposer shall be

liable for the replacement and installation costs of all CCSO-owned equipment that is unaccounted for or has unaccounted for damage in the closing inventory.

2.7.4 Food Service Equipment Maintenance and Repairs

The Proposer shall be responsible for providing, at its own expense:

- A. General maintenance to all dietary areas occupied and used by the Proposer.
- B. Proper preventative maintenance pursuant to manufacturer instructions and repair of the following CCSO-owned food service equipment for the life of the contract:
 - 1. All kitchen equipment, including exhaust systems, hoods, kitchen fire protection equipment, kettles, ovens, dishwashers, food service carts, and conveyor equipment.
 - 2. All electrical, heating and refrigeration units, including the compressors, that are used to service the CCDOC Central Kitchen, ODR, and within the preparation, service, receiving and storage areas.

The CCSO shall replace CCSO-owned food service equipment that has reached the end of its useful life, provided that the equipment was properly maintained and repaired by Proposer for the life of the contract.

2.7.5 Supplies, Small Wares, and Commodities

The Proposer shall provide all supplies and small wares used in performance of the contract, including, without limitation:

- A. Disposable eating utensils for each meal except authorized sack lunches;
- B. Serving utensils;
- C. Pots and pans;
- D. Paper products, including napkins;
- E. Plastic wrapping materials; and
- F. Service ware items, such as disposable trays.

Only supplies that comply with Cook County recycling and environmental ordinances shall be used. The Proposer shall purge and replace all damaged small ware items quarterly.

The Proposer shall provide all commodities, including foodstuffs, dry goods, canned foods, frozen foods, cereal, spices and the like, and shall draw all commodities in a first in, first out basis. To ensure proper stock rotation, all non-perishable food items will be marked with the color identifying the quarter it was received. The following colors shall be used to mark all non-perishable food items:

- A. First Quarter (January – March) marked with Red.
- B. Second Quarter (April – June) marked with Blue.

- C. Third Quarter (July – September) marked with Green.
- D. Fourth Quarter (October – December) marked with Yellow.

Proposer shall be presumed to be the owner of all supplies, small wares and food inventories used for this contract. Proposer shall be required to review the specifications and utilization of such supplies with the CCSO and obtain approval before such supplies may be employed at the CCDOC.

2.8. Sanitation and Pest Control

2.8.1 Sanitation

Proposer shall be responsible for cleaning and housekeeping in the food preparation, CCDOC Central Kitchen, ODRs, and all associated washroom and locker-rooms, service and storage areas, elevators, and will keep such areas in a clean and sanitary condition, and in conformity with all applicable federal, state and local regulations and requirements.

- A. Proposer shall be responsible for providing cleaning, janitorial and housekeeping materials. Such must comply with the CCSO's rules, regulations, policies and procedures, and with County, State and Federal EPA and food service laws and regulations.
- B. The Proposer shall establish hazardous chemical logs and comply with all applicable CCSO rules, regulations, policies and procedures concerning the use, storage and handling of hazardous substances.

2.8.2 Pest Control Services

The Proposer must develop and maintain an effective program for extermination and control of vermin and rodents, which includes pest control services to be performed on a weekly basis for the entire CCDOC Central Kitchen, ODR, and any and all food service and dining areas.

The Proposer must coordinate its pest control program with the vermin control programs conducted by the CCSO's contracted pest control vendors.

2.9. Cost Accounting System & Reporting

The Proposer shall provide a computerized Food Service Management Cost Accounting System ("Accounting System"). The Accounting System shall record and itemize all meals ordered, prepared, and delivered by the Proposer for the term of the contract. The CCSO retains sole ownership of the CCSO's data contained within the Proposer's proposed Accounting System. This data is proprietary and confidential and shall not be used by the awardee for any purpose other than what is required by this RFP.

Maintenance of all provided software and hardware shall be the responsibility of the Proposer for the duration of the contract terms, including renewal years.

Technical Proposal must address how Proposer's Accounting System will meet the following requirements:

- A. Electronically track all meal ordering, daily meal order reports, billing, inventory, small wares, supplies, uniforms, and food service operation activity up to and including menu preparation and compliance, recipe preparation, food production, equipment maintenance and repair, and other budgetary activity.

- B. Interface with the CCSO Jail Management System and any subsequent versions for the life of the contract. The interface must include, but is not limited to, continuous synchronization of data concerning CCDOC detainee meal specifications with individual booking profiles. The data must be transferred in the following format:

1. Booking Id (nvarchar(100))
2. Inmate ID (nvarchar(100))
3. Inmate Name (nvarchar(100))
4. Bed assignment (nvarchar(100))
5. Meal plan Category (nvarchar(100))
 - i. Administrative
 - ii. Religious
 - iii. Regular
 - iv. Medical
 - v. Work Detail Supplied
6. Meal Plan Description (nvarchar(100))
7. Effective Date (Datetime)
8. End Date (datetime)
9. Approved By (nvarchar(100))
10. Date booked (datetime)
11. Division Assigned (nvarchar(100))
12. Tier Assigned(nvarchar(100))

- C. Electronically track all ODR meals. CCSO staff ordering ODR Meals must present identification reflecting authorization to receive a staff meal, and Proposer must register staff meal service by scanning proximity cards, including 37-bit HID cards. Proposer must be able to sustain an integration between the CCSO's employee proximity card table and Proposer software, in order to ensure that any changes to employee proximity numbers will be updated. The proposed solution must be able to integrate the Sheriff's Office's active employee tables, which maintain up to date employee information.

1. The Proposers system must be able to accept 37 BIT HID proximity cards. Below are the integration fields/frequencies.
 - Type: Flat File Excel format
 - File Name: ODR_Proxy.xls
 - Schedule: 4 times daily at: 4:45am, 11:45am, 5:45pm, 11:45pm

Field Name		Field Type	Notes
EmployeeID		Int	Payroll ID
EmployeeName		Varchar(100)	Employee Full Name; {Last}, {First}
Prox_Number		Varchar(30)	ID Card number
CCSOUI		Varchar(9)	Unique User ID

Active_Flag		Bit	Active indicator	Employee
-------------	--	-----	------------------	----------

2. The system must be able to account for staffing status changes and custom/ad hoc reporting as needed.
 3. Proposer must have data sent back to CCSO BOIT with employee purchasing information. Payment method is not required to be sent back to us, only information about employees utilizing the discount and date time of use. This is for auditing and validation. CCSO BOIT will need the ability to run custom/ad hoc reports and the system will need to provide daily automated reports to the CCSO BOIT.
- D. Record and track each staff meal ordered and delivered in CCDOC ODRs, including the individual employee that scanned for each meal, the date and time of the proximity scan, and all other data elements as directed by the CCSO.
 - E. The ability to determine the cost per meal under the contract, broken out by the type of meal and the recipient.
 - F. Ensure safeguards for computer hardware, software, and data access so as to comply with the IT Special Conditions set out in Appendix XV.
 - G. The ability to provide continued operation with minimum interruption as well as backup of all data in the event of server error(s).
 - H. The ability for CCSO to directly access all data stored in Proposer's Accounting System. CCSO BOIT will be granted direct access, via VPN or through integrations (API,SFTP, FTPS). CCSO will be able to query, or have Proposer create custom queries and send data back to CCSO BOIT on a schedule (automated jobs) based on operational needs. Individual payment information is not required for CCSO access.
 - I. Supply, install, and maintain, at no cost to the County, all necessary technology, equipment, including on-site computers/workstations, server, wiring, and any other technology and/or resources required for operation of Proposer's Accounting System for all food service locations. Proposer's technology must be adaptable to all computer software, wiring, programming and hardware upgrades as directed by the CCSO. Below is a list of basic requirements:

General Requirements (On-Premise Solution)	
Processor	Intel 8 th Generation Core i7 Quad Core Minimum
Memory	16GB
Chipset	Intel Q270 Chipset
Graphic Options	Integrated Intel HD Graphics 610/630 (Intel 8 th Generation)
Operating System	Windows 10 Enterprise 64bit
Networking	1 Gigabyte minimum

2.9.1 Technology Requirements

Software must have the following interoperability with the current Cook County Jail Management Information System ("CCOMS"):

- A. Ability to transmit data to the Proposers system via SFTP, FTPS
- B. Transfer of data must be encrypted
- C. BOIT can allow for direct connection via VPN
- D. Must connect to a 2016 or newer SQL Server database
- E. Must adhere to security standards from Sheriff ISO
- F. Must be able to accept data at 15 minutes intervals to account for housing and custody status changes
- G. Minimum Data elements
 - 1. Booking Id
 - 2. Inmate ID
 - 3. Inmate Name
 - 4. Bed assignment
 - 5. Meal plan Category
 - 6. Meal Plan Description
 - 7. Effective Date
 - 8. End Date
 - 9. Approved By
 - 10. Date booked
 - 11. Division Assigned
 - 12. Tier Assigned
 - 13. Date Discharged

Must be able to accept custody status changes in their ordering system to deactivate orders based on status changes.

2.9.2 Meal Services Reporting Requirements

The following reports must be transmitted electronically from the Proposer to the CCSO:

- A. Master Menus: Master Menus must be received within thirty (30) days of the award of this contract and annually thereafter upon the anniversary date of the contract award date.
- B. Monthly Usage Report: Usage Report Summary will be transmitted by the 10th of each month.
 - 1. The Monthly Usage Report will note usage of products, meals served, and average cost including monthly and year to date data.

2. Proposer will ensure the Monthly Usage Report is generated after all transactions (receivers and pulls) for the month are completed.
- C. Staff Roster: A complete roster of all employee names addresses and the date each employee begin work in their current position under this contract shall be kept in the Proposer's site office. The Staff Roster shall be updated and submitted electronically each month with the monthly billing reports to the CCSO by the 1st of each month. The Staff Roster must also include filled and vacant positions.
- D. Standard Operating Procedures: Standard Operating Procedures must be received within thirty (30) days of the award of this contract.
- E. Food Service Staff Meeting Minutes: Portions of those minutes that concern enforcement of CCSO policies, rules, regulations and terms of this agreement will be forwarded to the CCSO in the monthly report.
- F. Staff Training: A report of completed training and issued certificates will be submitted by the Proposer to the CCSO by the 10th day of the quarter (January, March, June and September).
- G. Detainee Training: A report of completion and issued certificates, if any, will be submitted by the Proposer to the CCSO by the 10th of each month for each of the following:
 1. Initial Job Orientation Training: Each detainee assigned to work in Food Service will receive initial job orientation training, which shall include equipment training.
 2. Food Handler Certification Training: Each detainee assigned to work in Food Service will acquire their Food Handler Certification during the course of their food service assignment.
- H. Daily and Weekly Cleaning Schedules: Cleaning schedules will be developed by the Proposer listing cleaning of areas and equipment in the CCDOC Central Kitchen, ODRs, storage areas, and dock areas that are required to maintain high levels of sanitation. Daily and weekly cleaning schedules will be developed and will list the specific cleaning assignment, day, and shift during which the work will be completed. Temporary modifications to the cleaning schedule may be made with the CCSO's approval.
- I. Budget Projection Report: The Proposer shall develop and provide a budget projection report to estimate food service requirements and as the main planning device for food service provided under this contract.
 1. The budget projection report will act as a statement of known requirements for the purchase of supplies at wholesale and for other favorable prices and conditions.
 2. The budget projection report will be prepared and submitted to the CCSO by the 15th day of:
 - i. December for the first fiscal quarter.
 - ii. March for the second fiscal quarter.
 - iii. June for the third fiscal quarter.
 - iv. September for the fourth fiscal quarter.

2.10. Quality Assurance & Control Plan

2.10.1 Quality Assurance Plan

A Quality Assurance and Control Plan to assure contract requirements are met shall be prepared by the Proposer and submitted with the proposal. The Quality Control Plan shall be maintained throughout the duration of the contract. Any amendments to the plan after the contract is awarded shall be submitted to the CCSO two (2) weeks prior to implementation for review and approval. The original plan and any future amendments shall include, but not be limited to the following:

- A. The Proposer shall describe the policy and procedure for dealing with errors, missing menu/food items on trays or in meal packages, and damaged food.
- B. The Proposer shall provide a plan for dealing with detainee complaints concerning Food Service products and services at CCDOC. The Proposer shall provide grievance statistics for current facilities under contract for containing the largest detainee populations. The Proposer shall include the facility contact name and phone number of the individual who can verify the reported statistics.
- C. The Proposer shall conduct a survey of ODR diners quarterly to assess the acceptability of the menus. The Proposer may make adjustments based upon the survey results with the approval of the CCSO, providing that said adjustments have no impact on the cost per meal.
- D. The Proposer shall be required to observe all rules and regulations regarding storage, preparation and serving of food in the ODR that they are required to observe in the CCDOC Central Kitchen. It is allowable for the Proposer to make adjustments based upon the survey results. Adjustments will be allowed only with CCSO approval, providing that said adjustments have no impact on the cost per meal.
- E. Proposer shall detail an inspection system covering all of the services required by the contract, including the methods of identifying and preventing deficiencies in the quality of service performed before the level of performance becomes unacceptable; especially meal service.

2.10.2 Meal Quality Assurance

In conjunction with the specifications under Section 2.10.1, the Proposer shall provide the following in order to ensure meal quality assurance:

- A. Whenever a menu is updated, upon approval the new menu shall be rotated thereafter on a monthly basis to ensure variety. There is no alteration to the menu but for specific “days” such as national holidays or religious holidays. These special menus are developed by the Proposer and approved by the CCSO.

2.10.3 Inspection of Services

All services performed, and all materials, supplies and equipment furnished or utilized in the performance of services, and all workmanship in the performance of services, shall be performed in a quality manner and shall be subject to inspection and test by the CCSO at any time during the performance of the contract. The Proposer shall provide full cooperation with any inspector directed by the CCSO or the County to determine the Proposer’s conformity with these specifications and the adequacy of the services agreed to. All findings submitted to the Proposer shall be responded to in writing.

Inspections by the CCSO may include inspection by the state, County or city department of public health or any other agency or party authorized or directed by CCSO to inspect the facility. All inspections by the CCSO shall be made in such a manner as not to interfere unduly with or delay the work.

2.11. Environmental Sustainability

2.11.1 Environmental Sustainability Plan

The CCSO recognizes the importance of protecting the natural environment through conservation and sustainable practices, and therefore aims to reduce the volume and toxicity of waste materials produced in the course of its day-to-day operations. The Proposer's work force shall perform services in such a manner as to conserve electricity, gas, water, and steam.

Proposer shall prepare an Environmental Sustainability Plan that describes the steps Proposer will take to perform the Contract in an environmentally sustainable manner. Proposer is encouraged to include innovative ideas to meet the goals of the CCSO.

The Environmental Sustainability Plan shall be maintained throughout the duration of the Contract. Any amendments to the plan after contract are awarded shall be submitted to the CCSO two (2) weeks prior to implementation for review and approval. The original plan and any future amendments shall include, but not be limited to the following:

- A. The Proposer shall provide a complete list of environmentally sustainable products that it intends to use or supply during performance of the Contract. For each product, the Proposer shall identify the product, brand/manufacturer, and environmental program or standard met.
- B. Proposer shall describe how it intends to conserve electricity, gas, water, and steam, as well as reduce the volume and toxicity of waste materials during performance of the Contract.
- C. The Proposer shall be required to participate and integrate with the various waste diversion and recycling programs operated by the CCSO, including efforts intended to divert and reduce food waste.
- D. Consistent with federal, state, and County standards, the Proposer shall utilize and recycle fibrous (paper and cardboard), plastic, metal and other materials that are recyclable, including food waste.

2.11.2 Recycling and Waste Management

In conjunction with the specifications under Section 2.11.1, the Proposer shall be responsible for the following:

- A. Consistent with federal, state, and County standards, the Proposer shall utilize and recycle fibrous (paper and cardboard), plastic, metal and other materials that are recyclable, including food waste.
- B. The Proposer shall at Proposer's expense, provide, utilize and install a paper recycling apparatus.
 - 1. The Proposer shall be responsible for maintenance and supplies to operate the aforementioned apparatus.

2. The Proposer shall provide recycling bins for pre-sorting recyclables, including but not limited to paper, plastic, and aluminum.
 3. The recycling apparatus is provided for the exclusive use of the Proposer for food service related commodities.
 4. The Proposer shall process all food service-related commodities in manner consistent with recycling industry standards.
 5. Recyclable materials must be processed consistent with recycling industry standards, i.e. cardboard broken down and baled, paper products baled, cans and plastic containers washed and crushed separately.
- C. The CCSO will thereafter have responsibility for disposal or recyclables and will claim any and all revenue resulting from recycling. The Proposer's Food Service Director shall participate in weekly facility inspections with the CCSO designee.
- D. The Proposer shall be responsible for waste management including the proper removal of trash and garbage from the facilities to receptacles located adjacent to the CCDOC Central Kitchen.
1. The Proposer shall at the Proposer's expense, provide for scavenger services for removal of all waste generated by the Proposer in the performance of its duties under this contract from CCDOC premises. Said scavenger services shall be performed under the supervision of the CCDOC.
 2. The Proposer shall be responsible to provide all garbage containers/bins. All bins must have lids and be kept on containers/bins at all times. Proposer will remove garbage whenever container/bins are full, at the end of a meal period or at the end of the day. All containers/bins must be kept clean at all times.

2.12. Good Food Purchasing Program

The Good Food Purchasing Program ("GFPP") is a metric based, flexible framework that encourages public institutions to procure food produced through values-driven purchasing standards, in order to support the development of a more resilient and equitable food supply chain and make healthy, affordable, fair, and sustainable food more widely available to all communities.

Pursuant to the Cook County Board of Commissioners' Resolution to "Adopt the Good Food Purchasing Policy" (Resolution #18-1650), set forth in Appendix VII, Proposer is required to comply with the GFPP and adopt the Good Food Purchasing Standards, which emphasize five value categories: Local Economies, Environmental Sustainability, Valued Workforce, Animal Welfare, and Nutrition.

2.12.1 Good Food Purchasing Implementation Plan

To assure GFPP requirements are met, a Good Food Purchasing Implementation Plan shall be prepared by the Proposer and submitted with the proposal. The plan shall be evaluated based on the Good Food Purchasing Standards and Scoring System set forth in Appendix VII.

The Good Food Purchasing Implementation Plan shall be maintained throughout the duration of the contract. Any amendments to the plan after the contract is awarded shall be submitted to the CCSO two (2) weeks

prior to implementation for review and approval. The original plan and any future amendments shall include, but not be limited to the following:

- A. Proposer shall detail how they will initially meet or exceed the baseline standard set forth in Appendix VII for each Good Food Purchasing Standard value category.
 1. The baseline standard for each value category can be found in on:
 - i. Local Economies – Appendix VII, page 4
 - ii. Environmental Sustainability – Appendix VII, pages 8-9
 - iii. Valued Workforce – Appendix VII, page 15
 - iv. Animal Welfare – Appendix VII, page 20
 - v. Nutrition – Appendix VII, pages 25-27
 2. If Proposer cannot initially provide product(s) meeting baseline standard(s), Proposer shall outline a plan to meet the standard(s) by the end of the first year of the contract.
- B. Proposer shall provide a sample Food Purchasing Data Report for each fruit, vegetable, meat/poultry, dairy, and grain product that it intends to use or supply during performance of the contract.
 1. Proposer shall be required to submit an annual Food Purchasing Data Report for each fruit, vegetable, meat/poultry, dairy, and grain product used or supplied during performance of the contract that year.
 2. Both the sample and annual Food Purchasing Data Reports must include the following data fields:

Data Field	Description	Example
Farm Name	Name of farm where product was grown	<i>Driftless Organics</i>
Farm location (city and state)	Location of farm where product was grown or sourced at the city level	<i>Soldiers Grove, WI</i>
Processor/ Shipper/ Manufacturer/ Broker/ Wholesaler	Detailed information pertaining to the shipper/processor/manufacture information (any or all of these to the greatest extent possible). Any individual line item may have more than one input here, so please provide any and all growers that line item was sourced from under this contract.	<i>Russ Davis Wholesale</i>
Processing or manufacturing location (city and state)	Location where product was processed or manufactured at the city level	<i>LaCrosse, WI</i>
Brand (if applicable)	Brand name under which product is sold or marketed	<i>Driftless Organics</i>

Product Code	Unique identifying code assigned to the product	35317
Product Code Assignment	System to which product code belongs (ex: UPC)	<i>Internal Classification</i>
Product description	Description of the product or product name	<i>SWEET POTATOES</i>
Pack size	Size of pack in which product was purchased	<i>40# carton</i>
Quantity	Number of units that were purchased	2
Quantity UOM	Unit of measurement corresponding with Quantity field (i.e. CS, EA, LB)	<i>EA</i>
Net weight per quantity (in lbs.)	Weight for each unit that was purchased, in pounds	<i>40 lbs.</i>
Total weight (in lbs.)	Total weight for all units purchased	<i>80 lbs.</i>
Cost per unit	Cost per unit that was purchased	<i>\$22.40</i>
Total cost	Total cost for all units purchased	<i>\$44.80</i>

- C. Proposer shall disclose and provide a detailed description of any local, State, or Federal labor and/or environmental violations for which the Proposer has been cited in the last five (5) years
- D. The Proposer shall work with the CCSO, the Cook County Department of Public Health, and supporting partner organizations to review and annually update its Good Food Purchasing Implementation Plan in order to continuously work toward a higher score under Good Food Purchasing Standards and Scoring System.

2.13. Non-Compliance

In the event that provided meals and/or meal service are affected by Vendor's late or non-performance of an obligation under Section 2 of this RFP, the Proposer shall be charged for any or all of the following costs:

- A. Any and all actual costs associated with non-compliance, including but not limited to, equipment maintenance or repair costs associated with late or non-performance of an obligation under Section 2.7 (Facilities and Equipment) and mitigation costs associated with late or non-performance of an obligation under Section 2.8 (Sanitation and Pest Control); and
- B. The actual cost of those meals affected on the first day of the late or non-performance of any obligation under Section 2 of this RFP; and
- C. An additional penalty of 10% of the cost of meals affected on the second day of the late or non-performance of any obligation under Section 2 of this RFP.

The amounts charged shall be deducted from the same monthly bill in which the late or non-performance of any obligation under Section 2 of this RFP occurred or the affected meals were ordered.

3. Current State

The current state does not include a seamless integration into our jail management system. There is an existing integration for employee 37 BIT HID cards. Reporting functionality is minimal and manual.

<i>SYSTEM</i>	<i>CHARACTERISTICS</i>
CCOMS Jail Management System	Microsoft Dynamics/MS SQL-based jail management solution. CCOMS and proposed solution will exchange data bi-directionally
MS SQL Database Infrastructure	Multiple MS SQL databases will consume various data elements from proposed solution
Azure AD	Proposed solution will need to read from Azure AD and update itself with regard to employee status
SMTP-based outbound email	Proposed solution must have capability to send email via smtp where required

4. Future State

Proposed solution will interface with the current CCOMS jail management solution via vendor-recommended method appropriate to solution. Proposed solution must provide method where multiple MS SQL databases can consume data from solution via vendor-recommended method appropriate to solution. Proposed solution must provide an interface to allow CCSO to develop multiple re-useable reports. This interface must provide the ability to automate running and delivery of these re-useable reports. This interface must also provide a method allowing CCSO users to construct and run reports on an Ad-hoc basis. The ideal interface will provide a method to convert Ad-hoc reports into re-useable automated reports.

The proposed solution must possess the capability to read user information from Microsoft's Azure AD. The proposed solution must possess the capability to update user information – including, but not limited to, user access to system based on user's Azure AD account status – and update itself to grant or deny access based on user's Azure AD account status.

The proposed solution must possess the capability to email notifications, information, and reports to identified individuals via smtp. This smtp solution interfaces with Microsoft Azure Exchange.

5. Proposed Solution

Please limit your response to a total of 30 pages for all subsections under '5. Proposed Solution,' combined.

Note that Cook County reserves the right to purchase software, hardware, network equipment or other components directly through its own Countywide contracts, unless such recommended items are unique, intrinsic to the proposal, and can only be acquired through the Proposer.

5.1. Solution Overview

Proposers should present a concise high-level overview of the proposed solution, including:

- A. System architecture diagrams for solution not located on CCSO Premises. It is understood that the equipment providing Point of Sale [POS] functionality will be located on CCSO premises. The POS systems must be included in the system architecture diagrams.
- B. For cloud-based solutions proposer must provide: 1) preferred cloud provider; 2) proposed cloud architecture; 3) security architecture required to protect all data held and transferred to/from proposed solution.
- C. Any required frameworks or other software solution environment support required by proposed solution.
- D. Minimum requirements for front-end and back-end modules.
- E. Interfaces and integration points.
- F. Third party hardware and software included in the proposal or necessary for the proposal.
- G. Other key elements that will help the County better understand your proposed solution.

5.2. Software Overview

Proposer should provide a detailed description of the product(s) and product versions being proposed. The response to this section must detail the system features and capabilities and indicate if these are native to the software or if integration with a 3rd party software is required or recommended.

5.3. Hosting and Platform Architecture Overview

The Proposer must give an overview of the hosting and platform architecture, including at a minimum:

- A. System Environments: All environments (production, development, and test) included in the proposal and any differences or limitations in the various environments.
- B. Shared Components of the System: All shared components of the System (e.g., network segments, back-up tapes, etc.).

If the proposal is a cloud-based or a hybrid cloud-local solution, the proposer must describe:

- A. Proposed service model (e.g., SaaS, PaaS, IaaS);
- B. Proposed patching and maintenance service model;
- C. Proposed cloud deployment model (CJIS compliance standards, found in Appendix XVI, must apply));
- D. Any third parties relied upon in the proposed solution (e.g., hosting provider);
- E. Proposer's rationale for its choice of cloud deployment model; and
- F. How the cloud model might impact the County's data security and BOIT CJIS compliance and associated costs

Any pricing must be stated by Proposer **in its separate pricing proposal.**

5.4. Integration/Interface

Proposers should state cost efficient and financially feasible integration points between the proposed system and the stated existing technologies as well as, the proposed phase/timeline for interface(s) to go live. This approach must clearly show all integration related costs, alternate integration costs models, and feasible and realistic integration recommendations.

Proposers must also provide information about any implementation where the proposed solution is interfacing with existing technologies.

6. Solution Requirements

Please limit your response to a total of 10 pages for all subsections under ‘6. Solution Requirements,’ combined.

6.1. Hardware and Equipment Requirements

If hardware or equipment is included in, or required by, the proposal, then the proposer must describe:

- A. Required hardware and equipment, including minimum specifications of each.
- B. Responsibility for purchasing all hardware and equipment (e.g., proposer or County).
- C. Responsibility for installation of all hardware and equipment (e.g., proposer or County).
- D. Ownership of all hardware and equipment.
- E. Procedures for acceptance, partial shipments and back ordered hardware and equipment.
- F. Warranties and any terms and conditions associated with the hardware and equipment.

6.2. Physical Environment Requirements

The proposer must describe all physical environment requirements, if any:

- A. Physical location requirements (e.g., cooling, space, connectivity, etc.).
- B. Cabling/wiring and whether the County or Proposer would be responsible for procuring.
- C. County’s additional power requirements for operating required hardware and equipment.

As stated in Section 5.1 above, it is expected that POS equipment will be located on CCSO premises. All back-end aspects of the proposed solution will be located off-premises, either as traditional hardware, a pure cloud solution, or a hybrid configuration.

6.3. Network Requirements

The proposer must describe all network and bandwidth requirements associated with the proposal:

- A. Normal Bandwidth Requirements: The proposer shall include a reasonable estimate of minimum bandwidth required for concurrent application access and data access for “normal” daily operational use for cloud, hybrid and/or on-premise systems. Proposer shall also provide its definition of “normal daily operational use.”
- B. Peak Bandwidth Requirements: The proposer shall include a reasonable estimate of peak volume/times for retrieval and uploading transactions.
- C. Typical Impact: The proposer shall include a reasonable estimate of the typical impact expected on the network post implementation.
- D. Other Network Requirements: The proposer should describe the optimal physical network infrastructure required to effectively mitigate latency and data speed issues. Please describe the vendor provided physical network infrastructure, connectivity testing and performance assurance.

7. Implementation, Development and Project Management Services

Please limit your response to a total of 30 pages for all subsections under ‘7. Implementation, Development and Project Managements Services,’ combined.

This RFP seeks a managed implementation accomplishing tangible deliverables by agreed dates within a joint project task list and timeline. Functional and technical priorities are defined in the *System Requirements Matrix (Appendix XVII)*.

Proposers are expected to propose a best-industry methodology and solution. Innovative ideas to meet the needs of the County in a timely manner are encouraged. The proposed plan of action should adhere to a leading industry *project delivery methodology* (e.g., agile, waterfall, etc.). The Proposer shall describe its methodology in detail in Section 7.1.

Proposer must comply with the County’s content management procedures for tracking progress and documents for the duration of the project via either the County’s SharePoint site or as otherwise agreed. In addition, the Consultant Proposer will submit written weekly or monthly status reports to the County, which may include: work accomplished, updated Gantt charts, production goals, accepted deliverables, meetings and minutes, status of risks, issues or problems, summaries of approved project changes, and invoicing and payment.

7.1. Overview of the Implementation Methodology

Proposers should depict its implementation strategy in a high level diagram/table and also include:

- A. Brief description of proposed methodology;
- B. Proposed project phases;
- C. Team roles, including subcontractors;

- D. Milestones;
- E. Critical success factors; and
- F. Assumptions.

7.2. Project Task List and Timeline

Limit this response to the project plan and related timeline. Proposers should provide detailed scope tasks/activities, organized in phases including, but not limited to, project management activities, key resources, and estimated hours per key activity. Microsoft Project files are acceptable as attachments but this section requires an easy to read format (do not insert long “black lines” for the last pages of MS project plans).

7.3. Assessment, Change Management and Reengineering Approach

Proposers should provide a detailed description of your team’s approach to assessing and reengineering the County’s current state, while concurrently executing a feasible and effective change management plan. This section should include at minimum:

- A. Assessment approach;
- B. Human change management approach;
- C. Reengineering approach;
- D. County responsibilities for each of the above; and
- E. Expected Deliverables. **Proposers must use the following format:**

<i>Key Activity</i>	<i>Deliverables</i>	<i>Key Personnel/Responsibility</i>	<i>Acceptance Criteria</i>
1. Assessment	1. 2. 3.		
2. Change Management	1. 2. 3.		
3. Reengineering	1. 2. 3.		
4. Other			

7.4. Requirements Validation and System Design/Configuration

Proposers should provide a detailed description of its approach to validating business and technical requirements, including at minimum:

- A. Business requirements validation approach and related steps;
- B. Technical requirements validation approach and related steps;

- C. System design approach and related steps; and
- D. Any other key activities.

For each of the above, the Proposer shall detail expected Deliverables, the Proposer's and County's respective responsibilities, and acceptance criteria. **Proposers must use the following format:**

<i>Key Activity</i>	<i>Deliverables</i>	<i>Key Personnel/Responsibility</i>	<i>Acceptance Criteria</i>
1. Business requirements validation	1. 2. 3.		
2. Technical requirements validation	1. 2. 3.		
3. System design	1. 2. 3.		
4. Other			

7.5. System Implementation and Configuration

Proposers should describe its build and release approach, including at minimum:

- A. Required level of effort based on the expected configuration and customization work;
- B. Software configuration approach including check-in and check-out procedures;
- C. Software development approach including check-in and check-out procedures;
- D. System configuration and development management (documentation) procedures; and
- E. Any other key activity.

For each of the above, the Proposer shall detail expected Deliverables, the Proposer's and County's respective responsibilities, and acceptance criteria. **Proposers must use the following format:**

<i>Key Activity*</i>	<i>Deliverables</i>	<i>Key Personnel/Responsibility</i>	<i>Acceptance Criteria</i>
1. Environment Set up	1. 2. 3.		
2. Software configuration	1. 2. 3.		
3. Software customizations	1. 2. 3.		

4. Requirements Traceability Matrix	1. 2. 3.		
5. As-built system documentation	1. 2. 3.		
6. Other			

7.6. Data Conversion and Migration

Proposers should describe the plan for migrating/converting data from existing systems. Please consider the following questions when providing a response:

- A. What County resources do you anticipate will be required for data migration and conversion?
- B. What are the County's responsibilities?
- C. What is your approach regarding definition of data mapping rules?
- D. How does your approach address extraction, transformation, staging, cleansing and validation?
- E. Is the County or vendor responsible for cleansing County data prior to migration?
- F. What strategies do you employ to conduct the final conversion process?

If any conversion or migration tasks require additional cost, the proposer shall state such costs **in its separate pricing proposal**. Data migration tasks must be reflected on the project plan and timeline.

7.7. Quality Assurance ("QA")

Proposers should provide a detailed description of the proposed QA methodology adhering to best practices and clearly identifying control tasks and testing required to transition functionally from one environment to the next (e.g. dev to prod). The County expects this section to include at minimum:

- A. High level proposed QA approach;
- B. Proposed testing and promotion process;
- C. Proposed user acceptance process; and
- D. Other key activities.

For each of the above, the Proposer shall detail expected Deliverables, the Proposer's and County's respective responsibilities, and acceptance criteria. **Proposers must use the following format:**

<i>Key Activity</i>	<i>Deliverables</i>	<i>Key Personnel/Responsibility</i>	<i>Acceptance Criteria</i>
1. High level QA approach	1. 2. 3.		

2. Testing & promotion	1. 2. 3.		
3. System Testing (i.e., integration, conversion, regression, usability etc.)	1. 2. 3.		
4. Test Plans/Case Development	1. 2. 3.		
5. User Acceptance Testing	1. 2. 3.		
6. Other			

It is the expectation and requirement of the County that the proposer shall complete system testing prior to County user acceptance testing (UAT). Proposer shall provide all documentation related to system testing for County verification, validation and approval prior to UAT.

7.8. Knowledge Transfer /Training and Transition (Cutover)

Proposers should describe the recommended knowledge transfer and change management methodology ensuring County staff participation from the onset of the project. Describe the County's responsibilities and related escalation procedures if/when County participation is not promptly identified. This plan should include at minimum:

- A. Knowledge transfer approach;
- B. End user training approach (including training location, format, total training hours, number of employees trained, timing and signoff process);
- C. Administrator training approach (including training location, format, total training hours, number of employees trained, timing and signoff process);
- D. Transition/cutover approach; and
- E. Rollout support approach (the County expects on-site support during rollout)

For each of the above, the Proposer shall detail expected Deliverables, the Proposer's and County's respective responsibilities, and acceptance criteria. **Proposers must use the following format:**

<i>Key Activity</i>	<i>Deliverables</i>	<i>Key Personnel/Responsibility</i>	<i>Acceptance Criteria</i>
1. Knowledge transfer	1. 2. 3.		
2. End user training	1. 2. 3.		

3. Administrator training	1. 2. 3.		
4. Transition	1. 2. 3.		
5. Rollout support	1. 2. 3.		
6. Other			

7.9. Contract Performance Review and Acceptance

Proposers should describe all expected contract performance metrics, an approach to collect and transfer all assets to the County, the required key staff to attend close out session(s), and expected close out activities. This close out plan should include at a minimum:

- A. List of all expected final documentation and respective acceptance criteria/process;
- B. Vendor performance review expectations;
- C. Final project lessons learned review expectations; and
- D. Sample schedule of performance credits for failing to meet SLA and project milestones.

8. Solution Ownership and Other Terms and Conditions

Please limit your response to a total of 5 pages for all subsections under ‘8. Solution Ownership and Other Terms,’ combined.

8.1. Data Ownership

If awarded, all County Data shall be and remain the sole and exclusive property of the County. The selected Proposer will treat County Data as Confidential Information. The selected Proposer will be provided access to County Data hereunder for the sole and exclusive purpose of performing its obligations under the resulting Agreement, including a limited non-exclusive, non-transferable right to transmit, process, and display County Data only to the extent necessary in the provisioning of the Services and not for the storage or recording of County Data. The selected Proposer will be prohibited from disclosing County Data to any third party without specific written approval from the County. The Selected Proposer will have no property interest in, and may assert no lien on or right to withhold County Data from Cook County.

“County Data” means any data, including metadata about such data and backup or other copies thereof, that the proposer or its subcontractors obtains or accesses for the purposes of performing its obligations under the its proposal; to the extent there is any uncertainty as to whether any data constitutes County Data, the data in question shall be treated as County Data.

8.2. Intellectual Property Ownership

Proposer's deliverables may be considered "works made for hire" or otherwise assigned to or owned by the County. Proposer must state its agreement or must state any objection to this section. Specifically, the Proposer must address intellectual property ownership individually with respect to each of the following in its proposal:

- A. Commercial-off-the-shelf software or software components;
- B. Software customizations;
- C. Database schemas;
- D. Workflows;
- E. Project plans;
- F. Documentation;
- G. Training materials; and
- H. Other Deliverables

8.3. Hardware and Software Licensing

The proposal shall include a clear, high-level, non-legalese explanation of its hardware and software licensing. At a minimum, the explanation shall answer the following questions:

- A. What type of hardware and software license will the County receive? For example, would the County own licenses after the term of the proposed agreement?
- B. Who are the licensors? For example, is the proposer reselling or integrating a third party's hardware or software?
- C. Are any conditions attached to the hardware or software licenses? For example, would the County's licenses cease if the County chose to end maintenance services?
- D. Do any licenses propose to limit the manufacturers' liabilities or the County's remedies?

In an appendix, the proposal shall attach complete copies of hardware and software licensing agreements related to the proposal.

8.4. Software and Hardware Warranties

The proposal shall include a clear, high-level, non-legalese explanation of its hardware and software warranties. At a minimum, the explanation shall answer the following questions:

- A. What type of hardware and software warranties will the County receive?
- B. What would the warranties cover? If defects only, how are defects defined?

- C. What would the warranties exclude?
- D. What would be the County's remedies under the warranties? Repair and replace or other?

In an appendix, the proposal shall attach complete copies of hardware and software warranties related to the proposal.

8.5. Other Terms and Conditions

If the proposer requires any additional terms, the proposal shall include a clear, high-level, non-legalese explanation of them. At a minimum, the explanation shall answer the following questions:

- A. Does the proposer intend to impose upon the County any additional terms and conditions, such as end user license agreements, acceptable use policies, terms of service, product use agreements, etc.?
- B. Does the proposer want to reference its terms and conditions via URL or change its terms and conditions at a later date? Or would the proposer include copies of the additional terms and conditions as exhibits to a contract with the County?
- C. Do any additional terms limit the proposer's liabilities or the County's remedies?
- D. Does proposer's system of managing revenue recognitions affect its proposal, including, but not limited to pricing, guarantees, warranty provisions, or compliance with laws?

In an appendix, the proposal shall attach complete copies of any additional terms and conditions related to the proposal, such as: acceptable use policies, terms of service, privacy policies, and other terms and conditions.

9. Solution Performance and Availability

Please limit your response to a total of 5 pages for all subsections under '9. Solution Performance and Availability,' combined.

9.1. Hosting Services

The proposal must describe any hosting services it offers, including:

- A. Description of services: Any necessary information not provided in the hosting and architecture overview.
- B. Subcontractors: Whether the proposer provides hosting services directly or through a subcontractor; if through a subcontractor, include an explanation of how the proposer ensures its subcontractor will meet requirements of a contract with the County.
- C. Data Storage Limits and Overages: The proposer shall clearly state all data storage limits associated with the System. Where exceeding such data storage limits would cause the County to incur additional cost, the proposer shall state such costs in its separate pricing proposal.

- D. Data Transfer Limits and Overages: The proposer shall clearly state all data transfer limits associated with the System. Where exceeding such data transfer limits would cause the County to incur additional cost, the proposer shall state such costs in its separate pricing proposal.

9.2. Support and Maintenance Service

The proposal must individually address each the following requirements and provide sufficient detail on whether and how it meets the following requirements:

- A. Multi-tiered support: The proposal must provide multiple tiers of support and must state whether the County is assumed to provide tier 1 support.
- B. Severity levels: The proposal must provide support and maintenance response proportionate to varying levels of incident severity.
- C. Multiple contact method: The proposal should provide for multiple methods of reporting an incident to the proposer.
- D. First-tier support scripts: If the proposer assumes that the County will provide Tier 1 support, and then the proposer shall deliver sufficient scripts and training to County help desk staff to adequately function as Tier 1 support.

The proposal must individually address the following service level agreements (SLAs) for support and maintenance services, including whether such SLAs are offered and any additional cost for the SLAs, and detail on such:

- A. Proposer's Response Time SLAs: The time it takes an End-User to connect with Respondent's contact center live representative. Respondent will provide toll-free telephone lines in adequate quantity to handle call volume; ACD system(s) to record call date, time and duration information; and electronic interfaces to all systems for monitoring and reporting.
- B. Proposer's Resolution Time SLAs: Resolution is the time elapsed from the initiation of the Help Desk Incident until Service is restored.
- C. Other SLAs: If Proposers offer additional SLAs, they should be included.

For each SLA, the proposer must:

- A. Detail on how proposer will enable the County to verify SLA compliance.
- B. Detail any tiering of SLAs, whether by severity or other classification.
- C. Whether Proposer offers specific and calculable service level credits, but Proposer must state any credits **in its separate pricing proposal**.

9.3. Data Access and Retention

Furthermore, the response must state whether Proposer will meet the following data-related system requirements:

- A. At all times, the County shall be able to receive County data, associated metadata, and reasonably granular subsets thereof, as well as any associated files or attachments, from the System in a useable, encrypted format.
- B. Upon termination of the contract and at the County's written request, the Proposer shall destroy County Data, including backups and copies thereof, according to NIST standards or as otherwise directed by the County.
- C. The System shall have the ability to retain County data in a manner that is searchable and capable of compliance with records retention laws and best practices.
- D. At no time may Proposer suspend or terminate County's access to County Data or the System for breach of contract or term or condition relating to the System without giving the County reasonable notice and opportunity to cure according to the County's dispute resolution process.

9.4. Business Continuity and Disaster Recovery

The proposal must individually address each the following requirements and provide sufficient detail on whether and how it meets the following requirements:

- A. Proposers must have an automated backup and recovery capability for the system and application, including incremental and full backup capabilities. Additionally, system backups must be accomplished without taking the application out of service and without degradation of performance or disruption to County operations.
- B. Proposers must be able to provide the service from at least two geographically diverse data centers that do not share common threats (e.g. the data centers cannot be in the same earthquake zone, likely hurricane path, same flood zone, etc.). The data centers must at a minimum meet Tier III standards for redundancy of power, telecommunications, HVAC, security, fire suppression and building integrity.
- C. Proposers must specify whether, in the event of a technology or other failure at the primary processing center, the alternate system will meet the following tiers, for which the County's use should be identical regardless of which location is processing the County's work:

Category	Alternate system characteristics
High Availability	Continuous operation without interruption or degradation in service.
Standard Availability	Available for County use within 48 hours with no degradation in service.
Non-Critical Availability	Available for County use within 96 hours with no degradation in service.

- D. Proposers must implement crisis management, business continuity and disaster recovery plans, subject to County approval, which the County will not reasonably withhold. These plans must outline how the proposer will support the County's recovery at the alternate site, including backup staff required to implement the plan in an emergency if the proposer's primary staff is unavailable. Such plans shall also include a minimum of annual testing in coordination with the County

- E. Proposers must specify the System’s proven RTO and RPO in case the primary site becomes unavailable.
- F. Proposers must specify whether the System will meet the following availability tiers, which tier, and must specifically describe how the System meets such tier:

Category	Availability	RTO	Characteristics & RPO
High Availability	99.982%	Intra-day	Typically involves data replication to a hot-site for each transaction or at short intervals, like 15 minutes.
Standard Availability	99.741%	24 to 48 Hours	Nightly tape backups shipped to a warm-site data center. System reestablished at time of disaster from tape. May lose up to one day of data.
Non-Critical Availability	99.671%	48 to 96 Hours	Nightly tape backups shipped to offsite warm or cold site data center. System reestablished at time of disaster from tape after more critical systems are restored. May lose up to one day of data.

Proposers must detail available performance credits offered for a failure to meet uptime, RTO and RPO requirements.

“Recovery Point Objective” or “RPO” means the point-in-time that systems and data must be recovered and may range from point-of-failure, which has minimal loss, to data backed up the previous night or previous week (e.g., point-of-failure, one hour of data, one day of transactions or paper work). “Recovery Time Objective” or “RTO” means the timeframe business functions must be recovered after a declared outage (e.g., 24 hours).

9.5. Transition Out and Exit Requirements

The proposal must describe its plan for transitioning Deliverables, County data, and any County intellectual property to the County at the termination of the proposed solution or services, including:

- A. How the aforementioned would be delivered to the County;
- B. For hosted solutions, the procedure to import County Data to internal site, and the County's responsibilities in the event the County would want to transition to on premise hardware;
- C. Whether the Proposer would assist in transition to the County or successor vendor;
- D. How County data in contractors possession would be destroyed after transition;
- E. All assumptions and requirements, such as required time for transition or County participation.

The Proposer must include any costs associated with transition out **in its separate pricing proposal**.

9.6. Transition of Commencement of Contract

The Proposer shall assume full operations within forty-five (45) days of contract award. The Proposer shall coordinate and cooperate with the CCSO and the existing Proposer to assure a smooth and orderly transition with uninterrupted food services. Immediately upon award of the contract, the Proposer shall name a Transition Manager who shall have responsibility for transition activities. Within ten (10) days of award of the contract, the Proposer shall submit a Transition Plan to the Executive Director for approval.

The plan shall include but not be limited to details for conducting inventories of on-site CCSO-owned equipment, hiring and staffing, menu plans, and coordination activity with outgoing Proposer. The Executive Director/designee may request any additional information determined necessary to assure smooth operation of the facility. The CCSO presumes that all supplies and small wares stored on-site are owned by the current Proposer.

9.7. Continuity of Service

Continuity of Service is critical to the CCSO. The successful Proposer must recognize this fact and upon expiration of contract agree to:

- A. Furnish phase-in training to a new Proposer.
- B. Exercise best efforts and cooperation for an orderly and efficient transition to a new Proposer.
- C. Negotiate in good faith a plan with the successor to determine the nature and extent of the phase-in, phase-out services required.

The plan shall specify a date for work described in the plan and shall be subject to CCSO approval. The current Proposer shall provide sufficient experienced personnel during the phase-in, phase-out period to ensure that the services called for in the contract are maintained at the required level of proficiency.

Upon expiration of this Contract, the current Proposer shall permit personnel to be hired by a new Proposer without penalty or charge to the CCSO, the employee or the new Proposer. The current Proposer shall also disclose necessary personnel records and allow the successor to conduct on-site interviews with those employees. If selected employees are agreeable to the change, the current Proposer shall release them at a mutually agreeable date and negotiate the transfer of their earned fringe benefits to the new Proposer.

The current Proposer shall be presumed to be the owner of all supplies, small wares, and food inventories used for the Contract. Proposer shall be free to negotiate with the successor Proposer as to any terms and conditions for sale or transfer of ownership.

10. Security and Compliance

Please limit your response to a total of 5 pages for all subsections under ‘10. Security and Compliance,’ combined.

10.1. CCDOC Security Terms and Conditions

In light of the security responsibilities of the CCDOC, the County reserves the right to observe Proposer’s operations, inspect Proposer’s facilities, and interview Proposer’s personnel. Proposer agrees to abide by any and all CCSO rules, regulations, policies, and procedures.

The CCSO shall be responsible for security both within and outside the CCDOC Central Kitchen, and shall be entitled to remove any or all detainee(s) at any time from the kitchen or food service assignment, if in his discretion the detainee(s) presence poses or creates a security risk. The CCSO shall be entitled to restrict inmate access to any location within the CCDOC.

The Proposer shall promptly notify the designated CCSO staff of any security problems or any supervision issues that may have a potential impact upon security. The CCSO shall provide copies to all applicable security rules, regulations, policies, and procedures to the Proposer.

10.2. Criminal Background Check

All Proposer's employees, sub-vendors, agents and representatives must obtain the appropriate credentials from the CCSO and submit to a background check before commencing work at the CCDOC. The CCDOC Non-Employee Credential Process is set out in Appendix IX.

The CCSO reserves the right to process a criminal records check on the Proposer, Proposer's employees, sub-vendors, agents and representatives and to disqualify any person from participating in this Contract if found unsatisfactory. Proposer shall provide all requested identifying information about new and/or existing employees, sub-vendors, agents and representatives as may be required by the CCSO as a condition of acceptance for a specific employee.

10.3. Key Control

The CCSO shall have control of all perimeter keys, locks and security. The Proposer shall have keys and access to those areas where foods are stored and processed. It is the CCSO's intent that the Proposer have control of and access to the CCDOC Central Kitchen and ODR locations, except for matters related to security, fire protection and building repair; in these specific instances, the CCSO shall have absolute control. Cost for replacement of lost keys and other costs related directly to security costs stemming from lost keys by the Proposer's employees shall be borne solely by the Proposer.

10.4. Delivery to the CCDOC

The Proposal shall provide that all foodstuffs, goods and other materials deliverable to the County shall be shipped to the CCDOC Central Kitchen, and enter the Cook County Department of Corrections through Post 8, 3029 South Sacramento Avenue, Chicago, Illinois, 60608.

Truck deliveries will be accepted before 2:30 p.m. on weekdays only. No deliveries will be accepted on Saturdays, Sundays, or holidays. No product shall be received or stored at Cook County facilities for use at any other facility or locations.

The Proposer shall pre-notify CCSO Security Staff of all deliveries in accordance with CCSO rules, regulations, policies, and procedures. CCSO Security Staff may inspect such deliveries with respect to quantities, quality, weights, composition, or any other matter relevant in the estimation of the CCSO.

The Proposer shall only use plastic pallets at the CCDOC. The use of wooden pallets in areas where detainees are located is strictly prohibited. The CCSO will only allow deliveries to be received on wooden pallets and then immediately transferred to plastic pallets in the receiving area.

The Proposer shall be responsible for ensuring that foodstuffs, goods, and materials be delivered in clean, intact containers. The CCSO shall reject items that do not meet with the above specifications.

The Proposer shall be solely responsible for ensuring that all items it is to provide under the Contract, *e.g.*, foodstuffs, goods, and other materials, that are delivered to the CCSO are of the correct quantities, weights, quality and temperature at point of receipt.

10.5. Data Security Controls

The proposal must give an overview of the System's software, hardware, and other controls supporting the System's data security (NIST and CJIS Compliance Standards).

The proposer must also provide a reasonably detailed explanation as to how the proposal protects the System and County Data within each of the following additional data security categories (NOTE: the County recognizes that reasonable descriptions of each security attribute below will vary in length, some attributes requiring little explanation, others not.) (If proposer determines any of the following requirements to be inapplicable, proposer shall state so and shall also state the basis for determining each such requirement to be inapplicable):

- A. Password configurations (e.g., complexity, aging, etc.);
- B. Authentication configuration (e.g., active directory, encrypted data exchange, hash, etc.);
- C. Encryption configurations (e.g., symmetrical AES-256, asymmetrical RSA 2048, etc.) for both data at rest and data in motion;
- D. Logging/Auditing capabilities (e.g., verbose user tracking and reporting, etc.);
- E. Logs must be exportable to third party log aggregators;
- F. Physical security (e.g., 24-hour security, alarms, restricted access, etc.);
- G. Personnel security (e.g., extensive background checks, annual recheck, etc.);
- H. Web Application configurations (e.g., SQL injection protection, buffer overflow, etc.);
- I. Network transmission security (LAN and VPN); and
- J. Data that is to be transmitted off-site must be encrypted end to end.

Lastly, the proposer shall confirm that, under its proposal, all data-at-rest will not be stored outside of the continental United States.

10.6. Secure Development and Configuration Practices

The Proposer must describe its application development and configuration practices and how they will reasonably protect the security, confidentiality and privacy of County data and any individuals who may be considered data subjects as to the solution.

The Proposer should state whether it will adhere to the following guidelines: Microsoft Secure Coding Guidelines for the .NET Framework, CERT Secure Coding Standards, OWASP Secure Coding Principles, privacy by design principles, and the Federal Trade Commission's Fair Information Practice Principles.

10.7. Compliance Requirements

The proposer must provide sufficient detail on whether and how the proposal possesses data security controls that comply with (If proposer determines any of the following requirements to be inapplicable, proposer shall state so and shall also state the basis for determining each such requirement to be inapplicable):

- A. HIPAA, HITECH and the rules promulgated thereunder;
- B. Payment Card Industry standards, including but not limited to PCI DSS and PCI PA-DSS;
- C. 28 CFR 20 and the FBI's CJIS Security Policy;
- D. IRS Publication 1075;
- E. NIST 800-53, as revised; and
- F. ISO 27001/27002, as revised.

10.8. Incident Response Requirements

Proposer may include a full Incident Response Policy and/or related Plan as an attachment. In response to this section, the proposal must state the Proposer's approach to meeting the following data security incident response requirements:

- A. Maintenance of the Proposers' Incident Response Plan.
- B. Conformance of such plan to Illinois Personal Information Protection Act and the breach notification laws of the fifty states.
- C. Cook County's rights of review, approval and reasonable modification to Proposer's incident response plan.
- D. Proposer's approach to provide detailed reports on the nature of incidents and identified data lost or stolen.
- E. Proposer must describe its plan to address security incidents and data breaches in alignment with the following requirements. For events within the control of Proposer, the Proposer is expected to:
 - 1. Immediately notify the County of incidents and breaches.
 - 2. Identify immediate plan of action to mitigate further incident progression.
 - 3. Identify protection measures for affected individuals.
 - 4. Provide outbound and inbound incident-related communications, as requested and directed by the County.

10.9. Audit Requirements

The proposal must individually address each the following requirements and provide sufficient detail on whether and how it meets the following requirements:

- A. The proposer will provide SOC 2, Type 2 reports to the County annually or upon request.
- B. The proposer will provide corrective action plans or actions taken to resolve any exceptions, material weaknesses and/or control deficiencies identified in the SOC report.
- C. The County will have the right to access and audit proposer's system and hosting.
- D. The County will have the right to request reasonable adjustments at the proposer's expense where those requests are based upon audit findings pertaining to the System or Hosting.

11. Instructions to Proposers

11.1. Instructions

This RFP provides potential proposers with sufficient information to enable them to prepare and submit proposals. This RFP also contains the instructions governing the submittal of a proposal and the materials to be included therein, including the County requirements, which must be met to be eligible for consideration. All proposals must be complete as to the information requested in this RFP in order to be considered responsive and eligible for award, including all attached appendices. Proposers providing insufficient details will be deemed non-responsive. The County is not obligated, either to purchase the full services or the products proposed by the proposer, nor to enter into an agreement with any one proposer.

11.2. Availability of Documents

The County will publish their competitive bid, RFP, and other procurement notices, as well as award information, at:

<http://legacy.cookcountygov.com/purchasing/bids/listAllBids.php>

Interested suppliers should note that, unless otherwise stated in the bid or RFP documents, there is no charge or fee to obtain a copy of the bid documents and respond to documents posted for competitive solicitations. Proposers intending to respond to any posted solicitation are encouraged to visit the web site above to ensure that they have received a complete and current set of documents. Some procurement notices may provide a downloadable version of the pertinent documents and any amendments to them, which will be available to suppliers after they have completed a simple registration process. Additionally, some notices may permit a supplier to submit a response to a posted requirement in an electronic format.

Any proposers receiving a copy of procurement documents from a bid referral service and/or other third party are solely responsible for ensuring that they have received all necessary procurement documentation, including amendments and schedules. The County is not responsible for ensuring that all or any procurement documentation is received by any proposer that is not appropriately registered with the County.

11.3. Pre-Proposal Conference Call and Mandatory Site Visit

The County will hold a Pre-Proposal conference on the date, time and location indicated below. Representatives of the County will be present to answer any questions regarding the services requested or proposal procedures. Prospective Proposers will respond to the contact person listed on the front cover of the RFP **at least three business days prior to the Pre-Proposal Conference providing the following information: Attendee Name, Title, Company Name, Company Address, and additional documents as outlined in Appendix IV. See Appendix IV for Site Visit information/procedures.**

Mandatory Pre-Proposal Conference Call

Tuesday, December 15, 2020 at 12:00 PM CST

Please join using the link below:

https://teams.microsoft.com/l/meetup-join/19%3ameeting_ZjBiMDlkMzItZmVmZS00NTVILWFiZTItNGVIYzVhMzk3MzBj%40thread.v2/0?context=%7b%22Tid%22%3a%228b4d55ae-6db4-4e05-a85c-59d6a256cd6e%22%2c%22Oid%22%3a%22099d9406-018d-414b-8e8e-8a1d089320f3%22%7d

11.4. Mandatory Site Visit

The County will hold a Mandatory Site Visit on the date, time and location indicated below. Prospective Proposers will respond to the contact person listed on the front cover of the RFP **at least four business days prior to the Pre-Proposal Conference providing the following information: Attendee Name, Title, Company Name, Company Address, and additional documents as outlined in Appendix IV. See Appendix IV for Site Visit information/procedures.**

Mandatory Site Visit

**Wednesday, December 16, 2020 - Times will be scheduled with each vendor
2750 S. California
Chicago, IL 60608**

11.5. Clarifications

Questions regarding this RFP will be submitted in writing to the contact person listed on the cover page of this RFP no later than December 23, 2020 at 12PM (noon).

11.6. Submitting the Proposal Package

The Proposal and the Pricing Proposal shall be submitted to the OCPO electronically as per the instructions in Appendix III-Instructions for Submitting an Electronic Bid/Proposal/Qualification. OCPO will not accept hardcopy proposals. The Proposer remains responsible for ensuring that its Proposal is received at the time, date and manner specified. The County assumes no responsibility for any Proposal not so received. **Late Proposals will not be accepted.**

11.7. Uniformity

To provide uniformity and to facilitate comparison of Proposals, all information submitted must clearly refer to the page number, section or other identifying reference in this RFP. All information submitted must be

noted in the same sequence as its appearance in this RFP. The County reserves the right to waive minor variances or irregularities.

11.8. Proposal Material

The Proposal material submitted in response to the RFP becomes the property of the County upon delivery to the Office of the Chief Procurement Officer and will be part of any contract formal document for the goods or services which are the subject of this RFP.

11.9. Addenda

Should any proposer have questions concerning conditions and specifications, or find discrepancies in or omissions in the specifications, or be in doubt as to their meaning, they should notify the Office of the Chief Procurement Officer no later than December 23, 2020 by 12:00pm (noon) to obtain clarification prior to submitting a Proposal. Such inquiries must reference the proposal due date and the County RFP number.

Any clarification addenda issued to Proposer prior to the Proposal due date shall be made available to all proposers. Since all addenda become a part of the Proposal, **the Addendum Acknowledgement Form (found in Appendix XII) must be signed by an authorized Proposer representative and returned with the Proposal on or before the Proposal opening date. Failure to sign and return any and all addenda acknowledgements may be grounds for rejection of the Proposal.**

Interpretations that change the terms, conditions, or specifications will be made in the form of an addendum to the solicitation by the County. If issued, the County will post the addenda on the County website: <http://legacy.cookcountygov.com/purchasing/bids/listAllBids.php>. In the event there are any conflicts between the general terms and conditions and any special terms and conditions, the special terms and conditions shall take precedence.

11.10. Proposer's Responsibility for Services Proposed

The Proposer must thoroughly examine and will be held to have thoroughly examined and read the entire RFP document. Failure of Proposers to fully acquaint themselves with existing conditions or the amount of work involved will not be a basis for requesting extra compensation after the award of a Contract.

11.11. Errors and Omissions

The Proposer is expected to comply with the true intent of this RFP taken as a whole and shall not avail itself of any error or omission to the detriment of the services or the County. Should the Proposer suspect any error, omission, or discrepancy in the specifications or instructions, the Proposer shall immediately notify the County in writing, and the County will issue written corrections or clarifications. The Proposer is responsible for the contents of its Proposals and for satisfying the requirements set forth in the RFP. Proposer will not be allowed to benefit from errors in the document that could have been reasonably discovered by the Proposer in the process of putting the proposal together.

11.12. RFP Interpretation

Interpretation of the wording of this document shall be the responsibility of the County and that interpretation shall be final.

11.13. Confidentiality and Response Cost and Ownership

From the date of issuance of the RFP until the due date, the Proposer must not make available or discuss its Proposal, or any part thereof, with any employee or agent of the County. The Proposer is hereby warned that any part of its Proposal or any other material marked as confidential, proprietary, or trade secret, can only be protected to the extent permitted by Illinois Statutes.

11.14. Use of Subcontractors

The Proposer's response must include a description of which portion(s) of the work will be subcontracted out, the names and addresses of potential Subcontractors and the expected amount of money each will receive under the Contract. The County reserves the right to accept or reject any subcontractor if, in the County's sole opinion, it is in the best interest of the County.

11.15. MBE/WBE Participation Goals

Consistent with Cook County, Illinois Code of Ordinances (Article IV, Section 34-267 through 272), the County has established a goal that MBE/WBE firms retained as subcontractors receive a minimum of 25% MBE and 10% WBE participation of the overall estimated expenditures for this procurement. In an effort to continue to promote and expand the participation of certified MBE/WBE firms, the proposer shall make good faith efforts to utilize MBE/WBE certified firms as subcontractors. In its response, a proposer shall state the name(s) of the minority and women subcontractor(s) and the level of participation proposed for each firm to be awarded a subcontract and submit the MBE/WBE Utilization Plan Forms (included in this RFP in Appendix XIII) in a separate envelope (see Section 14.1 Number of Copies).

11.16. Proposer's Disclosure and Conflict of Interest

The Proposer must complete and return the enclosed "Economic Disclosure Statement & Forms" (Economic Disclosure Form included in this RFP in Appendix X) along with their proposal. In the event that further clarification is required on any of the information provided, the County reserves the right to make any necessary inquiry with a proposer for such purpose. Such inquiry, if made, may include a deadline by which time any necessary clarifying information must be submitted.

11.17. Cook County RFP Format

All proposers will use this solicitation format for submitting their proposal. Variations or exceptions from the specifications and general conditions should be submitted in writing. Such variations or exceptions may be considered in evaluating the offers received. Any exception taken must be noted in the space provided within this solicitation. Failure to comply with this requirement may cause a proposer's proposal to be considered "nonresponsive."

11.18. Pricing

All price and cost information requested in this solicitation should be provided by the proposer following the Pricing Instructions found in Appendix I of this RFP and utilizing the Pricing Template found in Appendix II of this RFP. While price is a factor in the evaluation of responses received, the relevant importance of price may vary based on the nature of the purchase and the related significance of other criteria as may be expressed elsewhere in this solicitation. In evaluating price, the County may give consideration to all cost of ownership factors relevant to determine the total final cost to the County, including but not limited to: administrative cost of issuing multiple awards. The County will be the sole determinant of the relevant and appropriate cost factors to be used in evaluating any Base or Alternate offers and/or Options.

11.19. Period of Firm Proposal

Prices for the proposed service must be kept firm for at least one hundred and twenty (120) days after the last time specified for submission of Proposals. Firm Proposals for periods of less than this number of days may be considered non-responsive. The Proposer may specify a longer period of firm price than indicated here. If no period is indicated by the Proposer in the Proposal, the price will be firm until written notice to the contrary is received from the Proposer, unless otherwise specified in this RFP.

11.20. Awards

The County may, at its discretion evaluate all responsive Proposals. The County reserves the right to make the award on an all or partial basis or split the award to multiple Proposers based on the lowest responsible proposers meeting the specifications, terms, and conditions. If a split award impacts the outcome of the project it must be so stated in the proposal.

11.21. Cook County Rights

The County reserves the right to reject any and all offers, to waive any informality in the offers and, unless otherwise specified by the Proposer, to accept any item in the offer. The County also reserves the right to accept or reject all or part of your Proposal, in any combination that is economically advantageous to the County.

11.22. Alteration/Modification of Original Documents

The Proposer certifies that no alterations or modifications have been made to the original content of this Bid/RFP or other procurement documents (either text or graphics). Any alternates or exceptions (whether to products, services, terms, conditions, or other procurement document subject matter) are apparent and clearly noted in the offered proposal. Proposer understands that failure to comply with this requirement may result in the proposal being disqualified and, if determined to be a deliberate attempt to misrepresent the proposal, may be considered as sufficient basis to suspend or debar the submitting party from future County Bid and RFP procurement opportunities.

11.23. Recycling

Packaging which is readily recyclable, made with recyclable materials, and designed to minimize potential adverse effects on the environment when disposed of by incineration or in a landfill is desired to the extent possible. Product(s) offered which contain recycled materials may be acceptable provided they meet all pertinent specifications and performance criteria outlined in this RFP. If the product(s) offered are manufactured utilizing recycled materials, identify the percentage composition and nature of the recycled content within.

12. Evaluation and Selection Process

12.1. Responsiveness Review

County personnel will review all proposals to ascertain that they are responsive to all submission requirements.

12.2. Acceptance of Proposals

Chief Procurement Officer reserves the right to reject any or all Proposals or any part thereof, to waive informalities, and to accept the Proposal deemed most favorable to the County.

12.3. Evaluation Process

An evaluation committee comprised of the County personnel will evaluate all responsive proposals in accordance with the evaluation criteria detailed below.

This evaluation process may result in a short-list of proposals. The evaluation committee, at its option, may request that all or short-listed proposers make a presentation, other customer testimonials, submit clarifications, schedule a site visit of their premises (as appropriate), provide a best and final offer, provide additional references, respond to questions, or consider alternative approaches.

12.3.1 Proposer Presentations

The County reserves the right to, but is not obligated to, request and require that each Proposer provide a formal presentation of its Proposal at a date and time to be determined. If required by the County, it is anticipated that such presentation will not exceed four (4) hours. No Proposer will be entitled to present during, or otherwise receive any information regarding, any presentation of any other Proposer.

12.3.2 Right to Inspect

The County reserves the right to inspect and investigate thoroughly the establishment, facilities, equipment, business reputation, and other qualification of the Proposer and any proposed subcontractors and to reject any Proposal regardless of price if it shall be administratively determined that in the County's sole discretion the Proposer is deficient in any of the essentials necessary to assure acceptable standards of performance. The County reserves the right to continue this inspection procedure throughout the life of the Contract that may arise from this RFP.

12.3.3 Best and Final Offer

The County reserves the right to request a Best and Final Offer from finalist Proposer(s), if it deems such an approach necessary. In general, the Best and Final Offer will consist of updated costs as well as answers to specific questions that were identified during the evaluation of Proposals. If the County chooses to invoke this option, Proposals will be re-evaluated by incorporating the information requested in the Best and Final Offer document, including costs, and answers to specific questions presented in the document. The specific format for the Best and Final Offer would be determined during evaluation discussions. Turnaround time for responding to a Best and Final Offers document is usually brief (i.e., five (5) business days).

12.4. Selection Process

Upon review of all information provided by shortlisted proposers, the evaluation committee will make a recommendation for selection to the Chief Procurement Officer for concurrence and submission to the County elected officials. The County reserves the right to check references on any projects performed by the proposer whether provided by the proposer or known by the County. The selected proposal will be submitted for approval to the County Board. The County intends to select a proposal that best meets the needs of the County and provides the best overall value. Upon approval of the selected Proposer, a contract will be prepared by the County and presented to the Selected Proposer for signature.

13. Evaluation Criteria

13.1. Responsiveness of Proposal

Proposer is compliant with all the submission requirements of the RFP.

13.2. Technical Proposal

Proposals will be reviewed and selected based on the following criteria in the table below:



Evaluation Criteria
Qualifications and demonstrated experience for the Proposer to successfully perform the services described and required in this RFP for the County, as evidenced by the successful implementation of similar services or programs in at least 3 large correctional facilities. Of those 3 facilities, at least one should service 2,000 inmates or more. (10%)
Quality of the proposed program plan as outlined in Section 2 (Scope) and demonstrated experience in providing Inmate Meal Food Service including food quality, meal preparation planning and meal packaging in a secure, complete, and timely manner. (30%)
Comprehensiveness of the proposed supplementary plans for, and demonstrated experience in, facility and equipment maintenance, pest control and janitorial services, environmental sustainability, etc. as outlined in Sections 2.7 (Facilities and Equipment), 2.8 (Sanitation and Pest Control), 2.11 (Environmental Sustainability), etc. (10%)
Comprehensiveness and quality of the proposed Good Food Purchasing Implementation Plan, including the plan for compliance with related food purchasing data collection processes, as outlined in Section 2.12.1 (10%)
Past history and references. Proposer shall include a listing of references with their proposal, indicating facility locations, name, and telephone number of facility contact person. This list should contain at least three (3) current references, preferably of a size and service complexity comparable to Cook County Department of Corrections. (5%)
Quality and ease of use of the comprehensive Technology plan that includes solutions for meal ordering, financial reporting/billing, and interoperability with the current Jail Management System. (10%)

13.3. Price Proposal

Price Proposal (Price will be evaluated separately for overall reasonableness.) (25%)

14.Submission of Proposal

14.1.Instructions for Submission

Number of Copies

Proposers are required to electronically submit their proposal no later than the time and date indicated in the RFP.

a. File #1 (“TECHNICAL PROPOSAL”) will contain documents as noted in Section 14.2 Submission Requirements. **Do not include any pricing information in this file.**

b. File #2 (“PRICING PROPOSAL”) will contain documents as noted in Section 14.2 Submission Requirements.

Time for Submission

Proposals shall be submitted no later than the date and time indicated for submission in this RFP. Late submittals may not be considered.

Format

Material should be organized following the order of the Submission Requirements (Section 14.2).

Complete Submission

Proposers are advised to carefully review all the requirements and submit all documents and information as indicated in this RFP, including all attached appendices. Incomplete proposals may lead to a proposal being deemed non responsive. Non responsive proposals will not be considered.

Packaging and Labeling

All electronically submitted files should be clearly marked to identify the 1) RFP solicitation number 2) Name of the proposer 3) Contents of the file (i.e. Pricing Proposal, Technical Proposal, MBE/WBE Utilization Plan Forms).

Timely Delivery of Proposals

The Proposal, including the Technical Proposal and the Pricing Proposal must be submitted electronically to Cook County, Office of the Chief Procurement Officer as per the instructions in Appendix II-Instructions for Submitting an Electronic Bid/Proposal/Qualification. Include the RFP number on any correspondence related to the Proposal.

Late Proposals

The proposer remains responsible for ensuring that its Proposal is received at the time, date, place, and/or office specified. The County assumes no responsibility for any Proposal not so received, regardless of the cause of delay.

Schedule of Revisions to RFP Schedule

Should the Proposer consider that changes in the County's RFP schedule are required; the Proposer shall submit a revised summary schedule with an explanation for the revision for the County's review. The County will be under no obligation to accept revised schedules.

14.2. Submission Requirements

Cover Letter – File #1

The cover letter shall be signed by an authorized representative of the Proposer. The letter shall indicate the Proposer's commitment to provide the services proposed at the price and schedule proposed.

Executive Summary – File #1

The executive summary should include a brief overview of the Commissary and Inmate Banking Services and the key personnel who will be responsible for the services to be provided. The Summary shall also identify the members of the team that comprise the Proposer. Indicate the organizational relationship of the team members and include an organization chart for the project.

Qualifications of the Proposer – File #1

Include a brief description of the organization's track record, including history, number of employees, number of years in business, and a list of projects relevant to this RFP. Provide a list of references where relevant projects were implemented. Include the name of the contact person, name of the organization, project dollar value, address, telephone number and email address. Please provide at least three (3) professional references, preferably with municipal government projects.

For each firm included in the proposal provide at least three (3) references with relevancy to the project scope. Additionally, provide accounts of yours for whom you have converted legacy or competitor data into your system format for account startup. The Contractor must list the facility name, contact name, and phone number of the facility(s) who are utilizing the feature on the Contractor's software.

Propose Plan of Action, Implementation and Solution – File #1

Provide a detailed proposed plan of action indicating how all requirements will be met and the methodology proposed recommendations and implementation plan to successfully meet the goals of the County. In addition, the proposed plan of action shall include key milestones, staff & schedule, and ability to deliver value with a solution evidenced by cost savings.

Key Personnel – File #1

Provide a chronological resume for each of the key personnel proposed. Each key personnel shall have three (3) references. In addition, provide the time commitment for each key personnel. Indicate the level of their commitment to other projects if any.

Subcontracting or Teaming – File #1

The proposer may be comprised of one (1) or more firms as to assure the overall success of the project. The firm shall identify each team member and specify their role. The Chief Procurement Officer reserves the right to accept or reject any of the team members if in the Chief Procurement Officer's sole opinion replacement of the team member, based on skills and knowledge, is in the best interest of the County.

Financial Status – File #1

Provide the audited financial statements for the last three fiscal years. Include the letter of opinion, balance sheet, schedules, and related auditor's notes.

Legal Actions – File #1

Provide a list of any pending litigation in which the proposer may experience significant financial settlement and include a brief description of the reason for legal action.

Conflict of Interest – File #1

Provide information regarding any real or potential conflict of interest. Failure to address any potential conflict of interest upfront may be cause for rejection of the proposal.

Contract – File #1

The Professional Services Agreement (included in this RFP in Appendix XI Cook County Contract Agreement) is provided for information only. Execution of the Contract is not required at the time the proposal is submitted.

In the event you disagree with the Contract provisions, submit any exceptions to the standard contract and include the rationale for taking the exception. If you are proposing alternate language, please include the language for consideration.

Appendix XII Addendum Acknowledgement Form – File #1

Other – File #1

Submit any information the Proposer deems pertinent to demonstrate its qualifications to perform the services being requested such as memberships in any professional associations.

Appendix II Pricing Proposal – File #2

Appendix XIV Identification of Subcontractor/Supplier/Subconsultant Form – File #2

Appendix X Economic Disclosure Statement – File #2

Execute and submit the Economic Disclosure Statement (“EDS”) (see Appendix X). In the event any further clarification is required on any of the information provided, the County reserves the right to make any necessary communication with the Proposer for such purpose. Such communication, if made, may include a deadline by which time any necessary clarifying information must be submitted.

Appendix IIIX MBE/WBE Participation – File #2

For each MBE/WBE certified firm proposed, provide the name of the MBE/WBE firm(s), level of participation, the role that the subcontractor(s) will perform, the type of services that it will provide, and a brief background and resumes of proposed personnel proposed and submit the MBE/WBE Utilization Plan Forms (see Appendix XIII). The County may only award a contract to a responsible and responsive proposer. In the event that the proposer does not meet the MBE/WBE participation goal stated by the County for this procurement, the proposer must nonetheless demonstrate that it undertook good faith efforts to satisfy the participation goal. Evidence of such efforts may include, but shall not be limited to, documentation demonstrating that the proposer made attempts to identify, contact, and solicit viable MBE/WBE firms for the services required, that certain MBE/WBE firms did not respond or declined to submit proposals for the work, or any other documentation that helps demonstrate good faith efforts. Failure by the proposer to provide the required documentation or otherwise demonstrate good faith efforts will be taken into consideration by the County in its evaluation of the proposer’s responsibility and responsiveness.

Appendix I – Pricing Instructions

1. Items Included in Cost Per Meal

“Cost per meal” shall be considered to include civilian labor; management; support services; supervision; profit and overhead; CCDOC Central Kitchen janitorial services, any and all taxes due or to become due on Proposer’s purchases or rentals; inventory control systems; security investigations; costs associated with employee labor relations; and any other Proposer costs necessary to perform the services of this Agreement.

2. Optional Items Included in Cost Per Meal

Where the County opts to provide any of the following items or services, said, items or services shall not be included in the Cost per meal: supplies, disposal supplies; small wares; food stuffs; equipment, equipment maintenance and repair; shall be considered to include civilian labor; management; support services; supervision; profit and overhead; food stuffs; Cost per meal may exclude the following items, at the option of the County: CCDOC Central Kitchen, and all related kitchen sanitation and janitorial services, supplies and equipment; eco-friendly packaging and disposable trays, supplies; small wares; equipment maintenance and repair; pest control; and information technology hardware and software.

3. Items Excluded from Cost Per Meal

The County shall solely provide the following items, which shall not be included in the Cost per meal: the cost to purchase or supply stationary capital equipment, i.e., machinery, refrigeration units, meat slicer, stoves, kettles, except for Proposer-owned specialty equipment, the cost of labor to deliver meals to detainees; the cost of building repairs; the cost of perimeter security; the cost to purchase food trays or distribution equipment costs, i.e., food delivery carts, all of which shall be borne by the County. Eco-friendly disposable trays will be utilized at the direction of the CCSO and will be supplied by the County.

- A. Specialized Equipment: To the extent that specialized equipment not provided by County is deemed by Proposer to be desirable, such equipment may be purchased by Proposer for performance of this contract, at no cost to Cook County. Such equipment shall be plainly identified to County as Proposer-owned equipment and shall remain the property of Proposer at the conclusion or termination of this Agreement. No such equipment will be recognized by County as Proposer’s property unless the equipment is identified in writing to the CCSO and the Purchasing Agent at the time the equipment is brought on site, by description, i.e. make, model description and serial number.
- B. The Proposer further agrees to destroy or remove from the CCDOC premises any item deemed to be rejected by the County and not to use in any form or manner the Rejected item as part of a meal delivered to the County, and where in the event such a Rejected item should be found to be part of a meal delivered to the County, the cost for any and all said meals shall be noted and immediately removed from that month’s billing to the County; and any delay in the delivery of meals affected by said meals shall result a penalty of 10% of the meal cost of those meals, which shall be noted and immediately removed from that month’s billing to the County.
- C. The Proposer further agrees that in the event that the Proposer delivers any meal more than fifteen minutes after the scheduled delivery time of said meal, the Proposer shall be automatically deemed not to have performed a provision of their Proposal and as described in this Request for Proposals by providing a late meal, which shall result a penalty of 10% of the meal cost of those late meals.

4. Annual Price Adjustment

The cost per meal shall remain firm for twelve (12) months or one (1) year following the award of the contract. Thereafter, either the Proposer or the County shall be entitled to request an annual price adjustment which shall be calculated in the manner provided for in this Section. The request for a price adjustment by the Proposer shall first be submitted to the Chief Procurement Officer and CCSO for consideration within sixty (60) days after the contract anniversary date of each year of the contract's term. In the event that the CCSO concurs with the price adjustment, it shall then be forwarded to the Chief Procurement Officer and the County Board of Commissioners for final approval, if necessary. The County shall notify the Proposer of its request for price adjustment within the same time period.

Price adjustment shall be based upon the Index for Food Away from Home, for all Urban Consumers for United States City Average, of the Consumer Price Index, as published by the United States Department of Labor, Bureau of Labor Statistics.

Price increase or decrease will be determined by dividing the current index for a contract anniversary month by the same prior year and month's index. All calculations will be carried to three (3) places only, with no rounding off to the next digit. An increase shall not exceed three percent (3%) annually from one adjustment period to the next.

EXAMPLE:

0.96 Current Meal Price

221.319 Current Index (anniversary month)

211.07 Last Year Month Index

PERCENTAGE INCREASE: 1.048

The Proposer shall not submit any penalty costs charged as a result of non-performance of the contract as part of its computation for costs per meal nor for any other form of payment from the County.

5. Payment

Payment to the Proposer will be made in arrears, within sixty (60) days after the close of each calendar month during the term of the Agreement. The sixty (60) days begins from the point that invoices are deemed acceptable and correct by the CCDOC. The Proposer shall prepare invoices and shall submit them to the CCSO with a certified statement of meals served as herein provided (including, but not limited to, breakfast, lunch, dinner, sack lunches, and any special detainee support services that were ordered by the CCSO) on a daily basis for the calendar month in question. Invoices shall be submitted within five (5) business days after the close of each calendar month.

There will be one point of contact for certification of meals served weekly for each of the following Sheriff's departments: Department of Corrections and Department of Court Services. This point of contact will be identified after the award of the new contract and will be incorporated into the Food Service Management Cost Accounting System.

The Proposer's certified statements shall be in a form acceptable to the County, including but not limited to a format that is part of a computerized Food Service Management Cost Accounting System, as required

under Section 2.9.1 (Technology Requirements) and is compatible with the current or future JMS utilized by the CCDOC, and shall reflect the exact number of meals prepared, the exact number of meals served, the cost of each meal, any extraordinary costs incurred, such as equipment repair, unplanned use of small wares, any cost savings as a result of food substitutions, spot buying or recycling, and categorized as follows:

- A. Actual number of CCDOC regular detainee breakfast meals served
- B. Actual number of CCDOC regular detainee bag lunch meals served
- C. Actual number of CCDOC regular detainee dinner meals served
- D. Actual number of Court Services lunches served by Court Call
- E. Actual number of detainee therapeutic meals served
- F. Actual number of detainee religious diet meals served

6. Optional non-CCDOC Mandated Meal Service (Meal Selection and Pricing)

The Proposer may propose an optional group of menu items, meal ordering, preparation and delivery plan, and pricing for non-CCDOC mandated meals that shall be determined jointly by the CCSO and the Proposer.

7. Commission Return for Optional non-CCDOC Mandated Meal Service

In the event that the Proposer submits the Optional Non-CCDOC Mandated Meals System proposal (as stated in Section 6 of this appendix), the Proposer's shall also propose a commission return for commissionable sales as described below:

- A. Food Service sales for Non-CCDOC Provided Meals and commissions will be paid for on a bi-monthly basis.
- B. A reasonable estimate of annual sales may be used to determine monthly commissions with actual sales and commissions computed at least yearly.
- C. Commissionable sales shall be construed as all moneys received from the sales of non-CCDOC mandated meals, less any refunds, allowances, or adjustments for returns, and applicable sale taxes.
- D. Final decisions on any disputes shall be made by the Chief Procurement Officer and CCSO.
- E. Detainees shall be charged all applicable Federal, State and County taxes. The Proposer can choose how to identify taxes to detainees. Proposer is responsible for remitting all applicable Federal, State and Local taxes.
- F. Proposer shall provide a monthly sales report to the CCSO no later than the 15th of each month. The monthly sales report must include the following information: (i) commissionable sales (ii) adjustments for credits and refunds; (iii) a cumulative total of commissionable sales and commissions paid to the County.

- G. The CCSO will not accept any proposals which offer additional commissions, funds, and or signing bonuses. It will not consider any proposal that has provisions for any other operation or program at the CCDOC or with Cook County.

8. Additional Pricing Terms and Conditions

- A. Meal item suggestions may be offered by either party.
- B. Items can be added or dropped only with the approval of the CCSO.
- C. Any item maybe rejected for security reasons; and as a result, all products containing glass, metal or alcohol or requiring additional cooking or heating are prohibited.
- D. Individual detainees may order only one non-CCDOC mandated meal per week. However, the CCSO reserves the right to increase or decrease the number of meals that may be ordered upon mutual agreement with the Proposer.
- E. Detainees may not order non-CCDOC mandated meals that are inconsistent with medically prescribed Therapeutic Meals, declared religious practices, or if they are prohibited from ordering for security or disciplinary reasons.
- F. All prices listed on the non-CCDOC mandated meals menu will include tax.
- G. Detainees will be charged all applicable Federal, State and Local Taxes. Proposer can choose how to identify taxes to detainees.
- H. The Proposer's proposed pricing will be firm for a period of twelve (12) months from the contract dated.
- I. Price increases thereafter without a reasonable explanation are prohibited. (Supplier increases would be an example of a reasonable explanation.)
- J. All menu items shall be priced competitively; consistent with comparable non-correctional retailers.

Appendix II – Pricing Template

Proposers are required to submit the attached pricing proposal separate from the technical proposal. In addition, include a breakdown of personnel rate card and the number and level of staffing for each task.

The pricing proposal must be submitted in electronic format.

If your company has specific, unique and/or innovative ideas to implement this system that are outside of the parameters defined on the pricing proposal, please provide your firm's recommendations on a separate sheet.

Section 1: Breakfast								
Meal Type		Price per meal	Annual Estimated Meals	Annual Total	Year 1 Total	Year 2 Total	Year 3 Total	Grand Total
General Meal (Breakfast) (DOC,SWIP,DRAD) - General			1,839,528	\$	\$	\$	\$	\$
General Meal (Breakfast) (DOC,SWIP,DRAD) - Therapeutic			317,554					
General Meal (Breakfast) (DOC,SWIP,DRAD) - Religious			3,416					

Miscellaneous One-time cost	\$
-----------------------------	----

Miscellaneous one-time cost Description	
---	--

Component Meal Costs		General Meal - Breakfast	General Meal - Therapeutic	General Meal - Religious
Food/Raw Materials	\$	\$	\$	\$
Wages/Labor	\$	\$	\$	\$
Administrative Costs	\$	\$	\$	\$
MBE/WBE Additional costs	\$	\$	\$	\$
Food waste allowance	\$	\$	\$	\$
Cook County - Owned Food Service Equip. Maint.	\$	\$	\$	\$
Cook County Food Service Facility Pest Control	\$	\$	\$	\$
Cook County Food Service Facility Maintenance	\$	\$	\$	\$
Small Wares, Supplies	\$	\$	\$	\$
Eco-Friendly Meal Packaging	\$	\$	\$	\$
Laundry Service for Inmate Uniforms or other Linens	\$	\$	\$	\$
Information Technology: Hardware & Software	\$	\$	\$	\$
Bulk Food Stuff Procurement	\$	\$	\$	\$
Profit Margin	\$	\$	\$	\$

Section 2: Lunch								
Meal Type		Price per meal	Annual Estimated Meals	Annual Total	Year 1 Total	Year 2 Total	Year 3 Total	Grand Total
General Meal (Lunch) (DOC,SWJP,DRAD) - General			1,782,168	\$	\$	\$	\$	\$
General Meal (Lunch) (DOC,SWJP,DRAD) - Therapeutic			316,490					
General Meal (Lunch) (DOC,SWJP,DRAD) - Religious			3,294					

Miscellaneous One-time cost \$

Miscellaneous one-time cost Description

Component Meal Costs	General Meal - Lunch	General Meal - Therapeutic	General Meal - Religious
Food/Raw Materials	\$	\$	\$
Wages/Labor	\$	\$	\$
Administrative Costs	\$	\$	\$
MBE/WBE Additional costs	\$	\$	\$
Food waste allowance	\$	\$	\$
Cook County - Owned Food Service Equip. Maint.	\$	\$	\$
Cook County Food Service Facility Pest Control	\$	\$	\$
Cook County Food Service Facility Maintenance	\$	\$	\$
Small Wares, Supplies	\$	\$	\$
Eco-Friendly Meal Packaging	\$	\$	\$
Laundry Service for Inmate Uniforms or other Linens	\$	\$	\$
Information Technology: Hardware & Software	\$	\$	\$
Bulk Food Stuff Procurement	\$	\$	\$
Profit Margin	\$	\$	\$

Section 3: Dinner								
Meal Type		Price per meal	Annual Estimated Meals	Annual Total	Year 1 Total	Year 2 Total	Year 3 Total	Grand Total
General Meal (Dinner) (DOC,SWJP,DRAD) - General			1,873,092	\$	\$	\$	\$	\$
General Meal (Dinner) (DOC,SWJP,DRAD) - Therapeutic			316,052					
General Meal (Dinner) (DOC,SWJP,DRAD) - Religious			3,246					

Miscellaneous One-time cost \$

Miscellaneous one-time cost Description

Component Meal Costs		General Meal - Dinner	General Meal - Therapeutic	General Meal - Religious
Food/Raw Materials	\$	\$	\$	\$
Wages/Labor	\$	\$	\$	\$
Administrative Costs	\$	\$	\$	\$
MBE/WBE Additional costs	\$	\$	\$	\$
Food waste allowance	\$	\$	\$	\$
Cook County - Owned Food Service Equip. Maint.	\$	\$	\$	\$
Cook County Food Service Facility Pest Control	\$	\$	\$	\$
Cook County Food Service Facility Maintenance	\$	\$	\$	\$
Small Wares, Supplies	\$	\$	\$	\$
Eco-Friendly Meal Packaging	\$	\$	\$	\$
Laundry Service for Inmate Uniforms or other Linens	\$	\$	\$	\$
Information Technology: Hardware & Software	\$	\$	\$	\$
Bulk Food Stuff Procurement	\$	\$	\$	\$
Profit Margin	\$	\$	\$	\$

Section 4: Boot Camp Meals									
Meal Type		Price per meal	Annual Estimated Meals	Annual Total	Year 1 Total	Year 2 Total	Year 3 Total	Grand Total	
Boot Camp Meal			286,558	\$	\$	\$	\$	\$	
Miscellaneous One-time cost		\$							
Miscellaneous one-time cost Description									
Component Meal Costs		Boot Camp Meals							
Food/Raw Materials		\$							
Wages/Labor		\$							
Administrative Costs		\$							
MBE/WBE Additional costs		\$							
Food waste allowance		\$							
Cook County - Owned Food Service Equip. Maint.		\$							
Cook County Food Service Facility Pest Control		\$							
Cook County Food Service Facility Maintenance		\$							
Small Wares, Supplies		\$							
Eco-Friendly Meal Packaging		\$							
Laundry Service for Inmate Uniforms or other Linens		\$							
Information Technology: Hardware & Software		\$							
Bulk Food Stuff Procurement		\$							
Profit Margin		\$							

Section 5: Sworn Staff Meals									
		Price per meal	Annual Estimated Meals	Annual Total	Year 1 Total	Year 2 Total	Year 3 Total	Grand Total	
Meal Type									
Sworn Staff Meals (CCDOC Division V and XI and Boot Camp)			70,232	\$	\$	\$	\$	\$	
Miscellaneous One-time cost		\$							
Miscellaneous one-time cost Description									
Component Meal Costs		Sworn Staff Meals (CCDOC Division V and XI and Boot Camp)							
Food/Raw Materials		\$							
Wages/Labor		\$							
Administrative Costs		\$							
MBE/WBE Additional costs		\$							
Food waste allowance		\$							
Cook County - Owned Food Service Equip. Maint.		\$							
Cook County Food Service Facility Pest Control		\$							
Cook County Food Service Facility Maintenance		\$							
Small Wares, Supplies		\$							
Eco-Friendly Meal Packaging		\$							
Laundry Service for Inmate Uniforms or other Linens		\$							
Information Technology: Hardware & Software		\$							
Bulk Food Stuff Procurement		\$							
Profit Margin		\$							

Section 6: Optional Non-CCDOC Provided Meal Service - Inmates, Staff, Designated Visitors									
Meal Type		Price per meal	Annual Estimated Meals	% Commission per meal	Annual Total	Year 1 Total	Year 2 Total	Year 3 Total	Grand Total
Optional Breakfast (Staff & Designated Visitor Only)			250,000		\$	\$	\$	\$	\$
Optional Lunch (Staff & Designated Visitor Only)			300,000		\$	\$	\$	\$	\$
Optional Dinner (Staff & Designated Visitor Only)			200,000		\$	\$	\$	\$	\$

Miscellaneous One-time cost \$

Miscellaneous one-time cost Description

Component Meal Costs		Optional Breakfast	Optional Lunch	Optional Dinner	Optional Dinner (Inmates)
Food/Raw Materials	\$	\$	\$	\$	\$
Wages/Labor	\$	\$	\$	\$	\$
Administrative Costs	\$	\$	\$	\$	\$
MBE/WBE Additional costs	\$	\$	\$	\$	\$
Food waste allowance	\$	\$	\$	\$	\$
Cook County - Owned Food Service Equip. Maint.	\$	\$	\$	\$	\$
Cook County Food Service Facility Pest Control	\$	\$	\$	\$	\$
Cook County Food Service Facility Maintenance	\$	\$	\$	\$	\$
Small Wares, Supplies	\$	\$	\$	\$	\$
Eco-Friendly Meal Packaging	\$	\$	\$	\$	\$
Laundry Service for Inmate Uniforms or other Linens	\$	\$	\$	\$	\$
Information Technology: Hardware & Software	\$	\$	\$	\$	\$
Bulk Food Stuff Procurement	\$	\$	\$	\$	\$
Profit Margin	\$	\$	\$	\$	\$

Section 7: Additional Information

1) What percentage discount would you provide for invoice payment at 20 days

2) What percentage discount would you provide for invoice payment at 30 days

3) Please describe your current rebate structure with food suppliers / food distributors (e.g. frequency, amount, etc...)

4) How would receiving USDA surpluses affect inmate meal pricing?

Appendix III – Instructions for Submitting an Electronic Bid/Proposal/Qualification

For electronic submissions, firms shall use the following link to submit Bids/Proposals/Qualifications electronically:

<https://www.cookcountyil.gov/service/online-solicitation-bid-submission>

Follow these steps to submit your electronic submission:

Step 1. Select the solicitation you are submitting a Bid/Proposal/Qualification for by clicking on the corresponding solicitation number. Once a solicitation number has been selected, it will be highlighted:

SOLICITATION INFORMATION

Note: * indicates a REQUIRED field.

Please Select Solicitation Number *

1901-18013 (Closes 4/29/20 – 3PM CST) ▲

2053-18202 (Closes 4/15/20 – 3PM CST) ▼

COMPANY INFORMATION

Step 2. Enter your company information:

COMPANY INFORMATION

Organization / Company Name *

Street Address *

City *

State *

Zipcode *

Step 3. Enter your company's point of contact information:

CONTACT'S INFORMATION
Contact First Name *
<input type="text"/>
Contact Last Name *
<input type="text"/>
Contact Email Address *
<input type="text"/>
Contact Phone Number *
<input type="text"/>

Step 4. Read the instructions and upload your Bid/Proposal/Qualification documents:

Solicitation Documents
<input type="button" value="Choose File"/> No file chosen
[Required] Files must be less than 75 MB . Allowed file types: pdf doc docx xls xlsx zip .

Note:

Use the section above to upload the required files for this Bid/RFP/RFQ. Please have ALL your files ready to upload when you submit your bid/Proposal, as you cannot save and continue later.

At least one file is required to be uploaded with your Bid, Proposal or Qualifications package. To download fillable PDFs for many of the forms included in the solicitation, please visit: <https://www.cookcountyil.gov/service/forms-affidavits>

The maximum file size is 75MB so Bids, Proposals, or Qualifications packages that exceed the allowable size limit may not upload properly. Please plan accordingly. If you have multiple files to upload, please put them together in a zip folder and upload the zip folder.

Successful submission of a Bid/Proposal/Qualification will result in an acknowledgement receipt e-mail sent to the address provided under point of contact information.

Appendix IV – CCDOC Site Visit Procedure

Site Visit Notification:

In order to obtain a 1-Day Pass, it is mandatory that every person attending the Field Inspection provide a copy of the attendees' current and valid state-issued Driver's License or Identification Card and a copy of their company business card enlarged to 150% to kelly.spencer@cookcountyil.gov by 12:00 p.m. (noon) December 10, 2020, for background check and to be approved by the Cook County Sheriff's Office

Tape measures and measuring wheels are permitted with an approved Tool List. Cell phones and cameras will not be permitted. Pictures of the site will be provided to the group as necessary. To obtain approval, submit Tool List via e-mail request at the same time as the 1-Day Pass to kelly.spencer@cookcountyil.gov. The 1-Day Pass and approved Tool List will be issued on the morning of the Mandatory Field Inspection.

Appendix V – General Meal Patterns

Breakfast

- 1 - 4 oz 10% fruit juice drink (Vitamin C fortified)
- 1 bowl or package of dry cereal
- 1 ea. hard cooked eggs (2 x per week)
- 2 slices wheat bread or 1 roll (equal to 2 slices of bread)
- 1 pastry, bagel or pop tart at least (4 x per week)
- 1 - 1 oz package of peanut butter (1 x per week)
- 1 - 1 oz cheese slice (2 x per week)
- 1 - 1 oz deli meat (2 x per week)
- 1 pc/package jelly

Lunch

- 2 sandwiches, consisting of:
- 3 oz. luncheon meat (variety)
- 4 slices wheat bread
- 2 packets of mustard or mayonnaise type dressing
- 1 bag chips (2 x per week)
- 1 package cookies (2 x per week)
- 1 package pretzels (3 x per week)
- 8 oz. fruit drink w/ vitamin C

Dinner

- 3 oz Meat (a whole muscle meat is to be served at least 2 x per month at a minimum)
- 1 cup potatoes, rice, noodles, beans, or other starch
- 1/2 cup coleslaw
- 1/2 cup vegetables
- 1/2 cup salad with 1 oz. dressing
- 2 slices wheat bread or a roll (equal to 2 slices of bread)
- 1 serving dessert (cookies 2 oz., or cake 1/70 ct. for full sheet, or 1/2 cup pudding or gelatin. Candy cannot be used as a dessert item)
- 1/2 oz margarine
- 8 oz milk (skim)
- 1 packet salt and pepper (when appropriate)

Appendix VI – Current Inventory of CCSO-Owned Equipment

Date of Inventory: December 20, 2019					
<u>Equipment Description</u>	<u>Qty</u>	<u>Manufacturer</u>	<u>Model Number</u>	<u>Serial Number</u>	<u>Life Year</u>
500 Gal Kettle	2	Chester/Jensen	70N-40	1401-P	10
100 Gal Kettle	1	Groen	FT100	86248	3
100 Gal Kettle	1	Groen	FT100	87104	3
100 Gal Kettle	1	Groen	FT100	86249	3
100 Gal Kettle	1	Groen	FT100	87099	3
200 Gal Kettle	1	Groen	INA/2-200	01699-3	3
200 Gal Kettle	1	Groen	INA/2-200	01698-1	3
140 Qt. Mixer	1	Hobart	V1401U	376377	8
Baxter Rotating Oven	1	Baxter	BXA2G	24-1056 519	5
Baxter Rotating Oven	1	Baxter	BXA2G	24-1056 521	5
Baxter Rotating Oven	1	Baxter	BXA2G	24-1056 520	5
140 Qt. Mixer	1	Hobart	V1401U	111028376	8
Cleveland Cabinet Steamer	1	Cleveland	PSMA	1.40E+12	5
Cleveland Cabinet Steamer	1	Cleveland	PSMA	1.40E+14	5
Cleveland Cabinet Steamer	1	Cleveland	PSMA	1.40E+14	5
Cleveland Cabinet Steamer	1	Cleveland	PSMA	1.40E+14	5
Rhino Insulated Carts	3	Rhino	N/A	N/A	4
Chuckwagon Insulated Cart	110	Cortech	N/A	N/A	1
Insulated Dinner Trays	*15000	Cortech	N/A	N/A	2
Chuckwagon Jr. Insulated Cart	10	Cortech	CWJ	N/A	8
Chuckwagon 2.0	15	Cortech	N/A	N/A	8
Cambro Insulated Cart	6	N/A	N/A	N/A	6
Prep Table, 2 Sided W/ Counter Top	3	N/A	N/A	N/A	10
Icemaker	1	Manitowoc	SY1405W	1101027388	6
Icemaker	1	Manitowoc	SY1405W	110102389	6
Ice Bin	1	Follet	950-48	C56950	6
Ice Bin	1	Follet	950-48	C56951	6
28ft Serving Line	1	N/A	N/A	N/A	8
Prep-Table/W Can Opener	1	N/A	N/A	N/A	10
Prep-Table With 2 Sinks	2	N/A	N/A	N/A	10
Prep Tables W/Sink	1	N/A	N/A	N/A	10
Dinner Service Line (2pc) W/ Roller Conveyors & Steam Wells	4	Cooks	NA	NA	10
3 Compartment Sink	1	N/A	N/A	N/A	10

Avtec Hood Ventilation System 60ft	1	Avtec	AIDC	34250	10
Taylor Dunn Vehicle	1	Taylor Dunn	CO-014-32	184827	10
Taylor Dunn Vehicle	1	Taylor Dunn	CO-014-32	184826	8
Taylor Dunn Vehicle	1	Taylor Dunn	CO-014-32	181202	8
Taylor Dunn Vehicle	1	Taylor Dunn	CO-014-32	184823	8
Taylor Dunn Vehicle	1	Taylor Dunn	CO-014-32	184822	8
Taylor Dunn Vehicle	1	Taylor Dunn	CO-014-33	184821	8
Cleveland Double Steamer	1	Cleveland	24CSM	1404000123	6
Prep-Table W/ Single Sink	1	N/A	N/A	N/A	10
Prep Table W/ Sink and Cabinet	1	N/A	N/A	N/A	10
Double Convection Oven	1	Hobart	NOHEC5	1830	6
Hood Ventilation System	1	Avtec	EIDC	34126	10
VCM-Food Processor	1	Hobart	N/A	N/A	3
Tool Cabinet	1	Carter Hoffman	SER200	N/A	4
Warmer (Hot Holding Cabinet)	1	FWF	N/A	N/A	4
1 Sided Prep Table With 2 Sinks	1	N/A	N/A	N/A	10
Prep Table W/ Sink	1	N/A	N/A	N/A	10
Prep Table W/ No Sink	1	N/A	N/A	N/A	10
3 Compartment Sink	1	N/A	N/A	N/A	10
Prep-Table W/ Sink	1	N/A	N/A	N/A	10
Tool Cabinet	1	N/A	N/A	36	6
Manual Meat Slicer	1	Hobart	J1-1510-278	HS610	10
Small Prep Table	1	N/A	N/A	N/A	10
Prep Table W/ Sink	1	N/A	N/A	N/A	10
80 Qt. Mixer	1	Hobart	L800D	11-1027-596	6
Prep-Table W/ Countertop	1	N/A	N/A	N/A	8
Prep Table W/ No Sink	1	N/A	N/A	N/A	10
Dishwasher	1	Hobart	FT1000ER	271196016	10
Dishwasher	1	Hobart	FT1000ER	271196017	10
Tray Pre-Scrap and Pulper	1	Hobart	WPS1200	10-0200436	1
Igloo	6	N/A	N/A	N/A	1
Stainless Steel Worktable W/ Sink	1	N/A	N/A	N/A	10
Chemical Storage Cages	2	N/A	N/A	N/A	5
Prep Tables W/ Sink Covered	2	N/A	N/A	N/A	8
Milk Cooler Evap Coil208/60/1	1	Refrigeration Design Tech.	RDMC8-4	T16G-18869	10
Milk Cooler Evap Coil208/60/1	1	Refrigeration Design Tech.	RDMC8-4	T16G-18868	10
Vestibule Cooler Evap Coil 115/60/1	1	Refrigeration Design Tech.	RDMC8-4	T16F17362	10

Meat Storage Evap Coil 115/60/1	1	Refrigeration Design Tech.	RDMC8-4	T16F17361	10
Meat Storage Evap Coil 115/60/1	1	Refrigeration Design Tech.	RDMC8-4	T15M13053	10
Safety Thaw Evap Coil 115/60/1	1	Refrigeration Design Tech.	RDMC8-4	T16F23348	10
Safety Thaw Evap Coil 115/60/1	1	Refrigeration Design Tech.	RDMC8-4	T16C07766	10
Vegetable Storage Evap Coil 115/60/1	1	Refrigeration Design Tech.	RDMC8-4	T16F18079	10
Vegetable Storage Evap Coil 115/60/1	1	Refrigeration Design Tech.	RDMC8-4	T16F17454	10
Daily Meat Evap Coil 115/60/1	1	Refrigeration Design Tech.	RDMC8-4	T16D22049	10
Daily Meat Evap Coil 115/60/1	1	Refrigeration Design Tech.	RDMC8-4	T16E87657	10
Daily Vegetable Evap Coil 115/60/1	1	Refrigeration Design Tech.	RDMC8-4	T16E08465	10
Process Food Evap Coil 115/60/1	1	Refrigeration Design Tech.	RDMC8-4	T16E82420	10
Process Food Evap Coil 115/60/1	1	Refrigeration Design Tech.	RDMC8-4	T16C11098	10
Process Food Evap Coil 115/60/1	1	Refrigeration Design Tech.	RDMC8-4	T16C21699	10
Process Food Evap Coil 115/60/1	1	Refrigeration Design Tech.	RDMC8-4	T16C21701	10
Meat Prep Room Evap Coil 115/60/1	1	Refrigeration Design Tech.	RDMC8-4	T16F16860	10
Meat Prep Room Evap Coil 115/60/1	1	Refrigeration Design Tech.	RDMC8-4	T16F16861	10
Vegetable Prep Evap Coil 115/60/1	1	Refrigeration Design Tech.	RDMC8-4	T16G05226	10
Vegetable Prep Evap Coil 115/60/1	1	Refrigeration Design Tech.	RDMC8-4	T16G05224	10
Vegetable Prep Evap Coil 115/60/1	1	Refrigeration Design Tech.	RDMC8-4	T16G05230	10
Ingredient Staging Evap Coil 115/60/1	1	Refrigeration Design Tech.	RDMC8-4	T16G05229	10
Ingredient Staging Evap Coil 115/60/1	1	Refrigeration Design Tech.	RDMC8-4	T16E87661	10
Test Kitchen Evap Coil 115/60/1	1	Refrigeration Design Tech.	RDMC8-4	T16G05225	10
Cart Holding Room Evap Coil 115/60/1	1	Refrigeration Design Tech.	RDMC8-4	T16E81715	10
Cart Holding Room Evap Coil 115/60/1	1	Refrigeration Design Tech.	RDMC8-4	T16E81716	10

Cart Holding Room Evap Coil 115/60/1	1	Refrigeration Design Tech.	RDMC8-4	T16F18082	10
Garbage Ref'd Room Evap Coil 115/60/1	1	Refrigeration Design Tech.	RDMC8-4	T16G20090	10
Sample Fridge Evap Coil 115/60/1	1	Refrigeration Design Tech.	RDMC8-4	T16E81871	10
Bulk Freezer Evap Coil 480/60/3	1	Refrigeration Design Tech.	RDMC4-4	T16G05258	10
Bulk Freezer Evap Coil 480/60/3	1	Refrigeration Design Tech.	RDMC4-4	T16G05259	10
Food Bank Freezer Evap Coil 208/60/3	1	Refrigeration Design Tech.	RDMC4-4	T15K03816	10
Food Bank Freezer Evap Coil 208/60/3	1	Refrigeration Design Tech.	RDMC4-4	T15K03818	10
Test Kitchen Freezer Evap Coil 208/60/3	1	Refrigeration Design Tech.	RDMC4-4	T16E82755	10
Food Bank Cooler 115/60/1	1	Refrigeration Design Tech.	RDMC8-4	T16F17453	10
Food Bank Cooler 115/60/1*	1	Refrigeration Design Tech.	RDMC8-4	T16F18072	10
Food Bank Cooler 115/60/1	1	Refrigeration Design Tech.	RDMC8-4	T16F17455	10
Food Bank Cooler 115/60/1*	1	Refrigeration Design Tech.	RDMC8-4	T16F18078	10
Food Bank Cooler 115/60/1	1	Refrigeration Design Tech.	RDMC8-4	T16F18077	10
Food Bank Cooler 115/60/1*	1	Refrigeration Design Tech.	RDMC8-4	T16F18071	10
Food Bank Condensers	7	Refrigeration Design Tech.	ADT-312	N/A	10
Bulk Freezer Condensers	2	Refrigeration Design Tech.	BHE-810	N/A	10
Food Bank Freezer Condenser	2	Refrigeration Design Tech.	LET-200	N/A	10
Test Kitchen Freezer Cond.	1	Refrigeration Design Tech.	LET-090	N/A	10
Milk Cooler Condensers	2	Refrigeration Design Tech.	BMA-450	N/A	10
Vestibule	1	Refrigeration Design Tech.	BMA-360	N/A	10
Meat Storage Cond.	2	Refrigeration Design Tech.	BMA-361	N/A	10
Safety Thaw Condensers	2	Refrigeration Design Tech.	ADT-130	N/A	10
Vegetable Storage Cond.	2	Refrigeration Design Tech.	ADT-312	N/A	10

Daily Meat Condensers	2	Refrigeration Design Tech.	ADT-120	N/A	10
Daily Vegetable Cond.	2	Refrigeration Design Tech.	ADT-370	N/A	10
Process Food Cond.	4	Refrigeration Design Tech.	ADT-130	N/A	10
Meat Prep Area Cond.	2	Refrigeration Design Tech.	LO-150	N/A	10
Vegetable Prep Cond.	3	Refrigeration Design Tech.	LO-165	N/A	10
Ingredient Storage	2	Refrigeration Design Tech.	LO-125	N/A	10
Test Kitchen Cooler Cond.	1	Refrigeration Design Tech.	ADT-120	N/A	10
Cart Storage Condensers	3	Refrigeration Design Tech.	ADT-180	N/A	10
Garbage Refrigerator	1	Refrigeration Design Tech.	ADT-104	N/A	10
Sample Fridge	1	Refrigeration Design Tech.	ADT-090	N/A	10
Work Tables 6' X 30"	2	N/A	N/A	N/A	10
Work Tables 6' X 24"	1	N/A	N/A	N/A	10
Work Table 4'X 36"	1	N/A	N/A	N/A	10
Work Table 24" X 24" W/ Wheels	1	N/A	N/A	N/A	10
Walk-In Freezer 13' X 8 '	1	Kolpak	Kolpak	410086286	10
Walk-In Cooler 13' X 8 '	1	Kolpak	Kolpak	410086286	10
Steam Table 5 Well	1	N/A	N/A	N/A	10
Refrigerated Sandwich Cooler	1	Delfield	N/A	N/A	10
Refrigerated Sandwich Cooler W/ 2 Drawer	1	Delfield	N/A	N/A	10
Tray Holder Stainless	2	Hatco	N/A	N/A	10
Conveyor Toaster	1	Hatco	N/A	N/A	10
Hood Ventilation System 6" sections	3	Captivaire Systems	5424 ND-2	NA	10
Double Convection Oven	1	Hobart	SCO-ES-10S	1.40523E+12	10
Electric Griddle 36"	1	Garland	NA	NA	10
Deep Fat Fryer Twin Side	1	Frialator	SE14R	E14HC047391	10
Ice Maker W/ Bin	1	Hoshizaki	KM134MAH	CO3276L	10
Shelving Racks	18	Metro	N/A	N/A	10
Televisions 43"	9	LG	N/A	N/A	10
Televisions 50"	1	LG	N/A	N/A	10
Grease Trap	1	Grease Interceptor	N/A	N/A	10
3 Compartment Sink W/ Pre-Wash and Drain Board	1	N/A	N/A	N/A	10

Mobile Work Table for Stand Mixer W/ Pan Rack	1	N/A	N/A	N/A	10
Grease Trap	1	Grease Interceptor	N/A	N/A	10
Grease Trap	1	Grease Interceptor	N/A	N/A	10
Cold / Heated Cabinet Twin Door Pass Through	1	Delfield Manitwoc	F160830	410086286	10
Beverage Display Refrigerator 3 Door	1	Delfield	DMER67-SLG	0.140516521	10
Grab and Go Refrigerated Cold Display	1	N/A	NA	NA	10
Commercial Coffee Brewer Twin	1	BUNN	CWTF - TWIN APS	TWIN 051054	10
Refrigerated Cooler Table 3 Door 5'	1	N/A	N/A	N/A	10
Hand Sink	1	Elkay	N/A	N/A	10
Hand Sink	1	Elkay	N/A	N/A	10
Hand Sink	1	Elkay	N/A	N/A	10
Hand Sink	1	Elkay	N/A	N/A	10
Hand Sink	1	Elkay	N/A	N/A	10
Conveyor Rack Dishwasher High Temp	1	Hobart	CL44E	85-10871T	10
Pre-Wash Table W/ Sprayer	1	N/A	N/A	N/A	10

Appendix VII – Cook County Good Food Purchasing Policy



Board of Commissioners of Cook County

118 North Clark Street
Chicago, IL

Legislation Details (With Text)

File #:	18-1650	Version:	2	Name:	TO ADOPT THE GOOD FOOD PURCHASING POLICY
Type:	Resolution	Status:			Approved
File created:	1/11/2018	In control:			Health & Hospitals Committee
On agenda:	1/17/2018	Final action:			5/16/2018
Title:	PROPOSED RESOLUTION				

PROPOSED SUBSTITUTE TO FILE 18-1650
(Health and Hospitals Committee 5/16/2018)

PROPOSED RESOLUTION

Sponsored By: JESUS G. GARCIA, JOHN A. FRITCHEY, STANLEY MOORE and RICHARD R. BOYKIN and LUIS ARROYO JR, JOHN P. DALEY, DENNIS DEER, BRIDGET GAINER, GREGG GOSLIN, SEAN M. MORRISON, TIMOTHY O. SCHNEIDER, PETER N. SILVESTRI, DEBORAH SIMS, LARRY SUFFREDIN and JEFFREY R. TOBOLSKI, County Commissioners

TO ADOPT THE GOOD FOOD PURCHASING POLICY

WHEREAS, Cook County strives to improve the health of all its residents through services and policies that promote health and well-being; and

WHEREAS, The Good Food Purchasing Program (GFPP) was developed in 2012 to encourage public institutions to procure food produced through values-driven purchasing standards and to support successful implementation through technical assistance and verification; and

WHEREAS, The Chicago Metropolitan Agency for Planning (CMAP) recommended the creation of sustainable local food systems in its Go To 2040 Comprehensive Regional Plan; and

WHEREAS, The Cook County Commission on Social Innovation, through its internal procedure reviewed, and now recommends, the adoption of a Good Food Purchasing Policy; and

WHEREAS, The Cook County Commission on Social Innovation found that sustainable food is ecologically sound, economically viable, and socially responsible; and

WHEREAS, The Cook County Commission on Social Innovation found that the health and well-being of residents can be supported by the creation of a sustainable local food system; and

WHEREAS, Good Food is defined by GFPP as food that is healthy, local, fair, sustainable and humane, with foods that meet the dietary guidelines for Americans, provide freedom from chronic ailment and are delicious and safe, and where participating food suppliers are evaluated and held accountable for ensuring fair compensation and fair treatment of their workers, and that those workers are free of exploitation, and where Good Food is available to purchase for all income levels and high-quality food is equitable and physically and culturally accessible to all, and where food is produced, processed, distributed, and recycled locally using the principles of environmental stewardship (in terms of water, soil, and pesticide management); and

WHEREAS, Good Food values prioritize nutrition, affordability, geography, and sustainable production practices including sound environmental practices, fair prices for producers, safe and fair working conditions for employees, and humane conditions for animals; and

WHEREAS, Good Food purchasing refers to the sourcing and purchasing of foods and beverages, and food and beverage service contracts, procured by County Departments and Agencies; and

WHEREAS, In participating in the Good Food Purchasing Program, Cook County will help support a regional food system that is ecologically sound, economically viable and socially responsible, and will have an impact on the availability of local, sustainable food; and

WHEREAS, Cook County adopted the Social Enterprise Preference to create opportunities for businesses that address social needs and employ people who are mentally, physically, economically or educationally disadvantaged including people with arrest and conviction records and those facing significant employment challenges.

WHEREAS, There is a need to preserve urban and peri-urban farm land with equitable minority community ownership and control; and

WHEREAS, There exists in the food and composting industries limited diversity in the ownership, production and distribution channels; and

WHEREAS, There are significant barriers to entry into the food industry at the ownership level, including access to capital and information, expertise and relationships, resulting in a need for capacity building for disadvantaged and under-capitalized businesses; and

WHEREAS, There are a number of tax credits available at the federal, state, county and city level to incentivize investment in distressed communities and to hire very low- income employees, employees with past criminal records, etc.; and

WHEREAS, It is recognized that the significant buying power of public institutions across the country can reform the food system, create opportunities for smaller farmers and low-income entrepreneurs of color to thrive, provide just compensation and fair treatment for food chain workers, support sustainable farming practices, reward good environmental stewardship including limiting food waste and increasing composting, and increase access to fresh and healthy foods; and

NOW THEREFORE BE IT RESOLVED, That Cook County embrace the Good Food Purchasing Program (GFPP) as a strategy to help improve our region's food system through the adoption and implementation of the Good Food Purchasing Standards, which emphasize the following values:

1. Local Economies - support small and mid-sized agricultural and food processing operations within the local area or region.

1.A. Priority Communities- Incentivize through GFPP bonus points purchasing food produced and/or processed for GFPP contracts from low-to-moderate income communities where at least 51% of households have incomes at or below 80% of the area median income (AMI), as defined by the U.S. Department of Housing and Urban Development. Priority will be given to communities that also have scores ranging between 30.1 and 82.7 on the University of Illinois at Chicago Great Cities Institute's Economic Hardship Index.

2. Environmental Sustainability -- Support farmers employing sustainable farming practices by using the least toxic crop protectants reducing the use of synthetic pesticides and fertilizers; utilizing antibiotics only when medically necessary; conserve and regenerate soil and water; protect and enhance wildlife habitat and biodiversity; and reduce on-farm energy consumption and greenhouse gas emissions.

3. Valued Workforce - provide safe and healthy working conditions and fair compensation for all food chain workers and producers from production to consumption

4. Animal Welfare - provide healthy and humane care for farm animals.

5. Nutritional - promote health and well-being by offering generous portions of vegetables, fruit, and whole grains; reducing salt, added sugars, fats, and oils; and by eliminating artificial additives.

BE IT FURTHER RESOLVED, that the following goals are also adopted and implemented as part of Cook County's participation in the Good Food Purchasing Program (GFPP) to address ongoing inequities and issues caused by unequal access to access and resources. Cook County Departments and agencies are tasked with developing multi-year action plans that will address these inequities by pursuing one or more of these possible strategies:

- * Encourage businesses to grow food organically and engage in bio-dynamic agriculture, developing incentives for Requests for Proposal reviews and other potential supports during the contracting period; and

- * Encourage prospective food vendors to invest in and hire from Priority Communities by: 1) developing bonus scores for Requests for Proposal reviews for prospective vendors demonstrating a track record of hiring and investing in such communities; and 2) assisting prospective vendors in navigating tax incentives and other financial programs designed to increase investment in disadvantaged communities; and

- * Encourage conveyance of publicly-owned vacant properties (land and buildings) to local minority owned and/or controlled social enterprises and/or community land trusts for urban agriculture and other food related enterprises in an equitable fashion by setting ownership goals for minority owned and controlled enterprises; developing incentives for Requests for Proposal reviews; exploring possibilities for technical assistance and financial assistance, including tax incentives; and

- * Encourage hiring people with arrest and conviction records by developing incentives for Requests for Proposal reviews, exploring options for technical assistance and financial assistance, including tax incentives; and

- * Engage local universities, social enterprises and small consulting firms with demonstrated expertise in providing technical assistance to emerging and/or disadvantaged businesses; and

BE IT FURTHER RESOLVED, that the Cook County Department of Public Health (CCDPH) convene a taskforce that includes all relevant Cook County Departments and Agencies involved in the procurement or service contracting of foods, including but not limited to, Offices under the President, the Office of the Chief Judge, the Juvenile Temporary Detention Center, the Office of the Sheriff, the Cook County Health and Hospital System, the Chicago Food Policy Action Council, the Center for Good Food Purchasing, and other relevant diverse stakeholders,

BE IT FURTHER RESOLVED, that the taskforce recommend flexibility within each of these five value categories and the following steps in support of the purchasing of Good Food and as a framework for guiding values-driven purchasing,

1. Communicate Good Food Purchasing Standards to appropriate suppliers, including distributors and foodservice companies, and ask them to share data that will help the County complete a baseline Good Food Purchasing assessment of food procurement practices within 12 months of the adoption of this resolution.

2. After the baseline assessment has been completed, develop and adopt an multi-year action plan with benchmarks to measure success towards Good Food Purchasing Standards, diversity goals, and programs to support emerging producers and suppliers from Priority Areas and diverse communities including accountability systems with appropriate vendors/distributors to verify sourcing commitments and assess current food procurement practices within 6 months; and

3. After the baseline assessment has been completed, establish supply chain accountability and traceability systems with vendors/distributors to verify sourcing commitments and assess current food procurement practices within 6 months; and

4. To the extent permitted by law, following the multi-year action plan, after the baseline assessment has been completed, incorporate Good Food Purchasing Standards into new procurement requests and contracts within 6 months; and

5. Seek resources as needed to staff and implement the Good Food Purchasing Standards; and

BE IT FURTHER RESOLVED, that the taskforce report its progress to the Health and Hospital Committee within 12 months of the adoption of this resolution, and then report annually on implementation progress; and

BE IT FURTHER RESOLVED, that the taskforce will host an annual public hearing where diverse community stakeholders and residents can ask questions and provide feedback on implementation, including due diligence reporting data to verify compliance, measure progress, and celebrate successes; and

BE IT FURTHER RESOLVED, that the taskforce will engage and encourage municipalities, townships, schools, hospitals and other entities within Cook County to adopt the Good Food Purchasing Policy.

Sponsors: JESÚS G. GARCÍA, LUIS ARROYO JR, RICHARD R. BOYKIN, JOHN P. DALEY, DENNIS DEER, JOHN A. FRITCHEY, BRIDGET GAINER, GREGG GOSLIN, STANLEY MOORE, SEAN M. MORRISON, TIMOTHY O. SCHNEIDER, PETER N. SILVESTRI, DEBORAH SIMS, LARRY SUFFREDIN, JEFFREY R. TOBOLSKI

Indexes:

Code sections:

Attachments:

Date	Ver.	Action By	Action	Result
5/16/2018	1	Health & Hospitals Committee	accept as substituted	Pass
5/16/2018	1	Board of Commissioners	approve as substituted	Pass
5/16/2018	1	Health & Hospitals Committee	recommend for approval as substituted	Pass
1/17/2018	1	Board of Commissioners	refer	Pass

PROPOSED RESOLUTION

PROPOSED SUBSTITUTE TO FILE 18-1650

(Health and Hospitals Committee 5/16/2018)

PROPOSED RESOLUTION

Sponsored By: JESUS G. GARCIA, JOHN A. FRITCHEY, STANLEY MOORE and RICHARD R. BOYKIN and LUIS ARROYO JR, JOHN P. DALEY, DENNIS DEER, BRIDGET GAINER, GREGG GOSLIN, SEAN M. MORRISON, TIMOTHY O. SCHNEIDER, PETER N. SILVESTRI, DEBORAH SIMS, LARRY SUFFREDIN and JEFFREY R. TOBOLSKI, County Commissioners

TO ADOPT THE GOOD FOOD PURCHASING POLICY

WHEREAS, Cook County strives to improve the health of all its residents through services and policies that promote health and well-being; and

WHEREAS, The Good Food Purchasing Program (GFPP) was developed in 2012 to encourage public institutions to procure food produced through values-driven purchasing standards and to support successful implementation through technical assistance and verification; and

WHEREAS, The Chicago Metropolitan Agency for Planning (CMAP) recommended the creation of sustainable local food systems in its *Go To 2040* Comprehensive Regional Plan; and

WHEREAS, The Cook County Commission on Social Innovation, through its internal procedure reviewed, and now recommends, the adoption of a Good Food Purchasing Policy; and

WHEREAS, The Cook County Commission on Social Innovation found that sustainable food is ecologically sound, economically viable, and socially responsible; and

WHEREAS, The Cook County Commission on Social Innovation found that the health and well-being of residents can be supported by the creation of a sustainable local food system; and

WHEREAS, Good Food is defined by GFPP as food that is healthy, local, fair, sustainable and humane, with foods that meet the dietary guidelines for Americans, provide freedom from chronic ailment and are delicious and safe, and where participating food suppliers are evaluated and held accountable for ensuring fair compensation and fair treatment of their workers, and that those workers are free of exploitation, and where Good Food is available to purchase for all income levels and high-quality food is equitable and physically and culturally accessible to all, and where food is produced, processed, distributed, and recycled locally using the principles of environmental stewardship (in terms of water, soil, and pesticide management); and

WHEREAS, Good Food values prioritize nutrition, affordability, geography, and sustainable production practices including sound environmental practices, fair prices for producers, safe and fair working conditions for employees, and humane conditions for animals; and

WHEREAS, Good Food purchasing refers to the sourcing and purchasing of foods and beverages, and food and beverage service contracts, procured by County Departments and Agencies; and

WHEREAS, In participating in the Good Food Purchasing Program, Cook County will help support a regional food system that is ecologically sound, economically viable and socially responsible, and will have an impact on the availability of local, sustainable food; and

WHEREAS, Cook County adopted the Social Enterprise Preference to create opportunities for businesses that address social needs and employ people who are mentally, physically, economically or educationally disadvantaged including people with arrest and conviction records and those facing significant employment challenges.

WHEREAS, There is a need to preserve urban and peri-urban farm land with equitable minority community ownership and control; and

WHEREAS, There exists in the food and composting industries limited diversity in the ownership, production and distribution channels; and

WHEREAS, There are significant barriers to entry into the food industry at the ownership level, including access to capital and information, expertise and relationships, resulting in a need for capacity building for disadvantaged and under-capitalized businesses; and

WHEREAS, There are a number of tax credits available at the federal, state, county and city level to incentivize investment in distressed communities and to hire very low- income employees, employees with past criminal records, etc.; and

WHEREAS, It is recognized that the significant buying power of public institutions across the country can reform the food system, create opportunities for smaller farmers and low-income entrepreneurs of color to thrive, provide just compensation and fair treatment for food chain workers, support sustainable farming practices, reward good environmental stewardship including limiting food waste and increasing composting, and increase access to fresh and healthy foods; and

NOW THEREFORE BE IT RESOLVED, That Cook County embrace the Good Food Purchasing Program (GFPP) as

a strategy to help improve our region's food system through the adoption and implementation of the Good Food Purchasing Standards, which emphasize the following values:

1. **Local Economies** - support small and mid-sized agricultural and food processing operations within the local area or region.
 - 1.A. **Priority Communities**- Incentivize through GFPP bonus points purchasing food produced and/or processed for GFPP contracts from low-to-moderate income communities where at least 51% of households have incomes at or below 80% of the area median income (AMI), as defined by the U.S. Department of Housing and Urban Development. Priority will be given to communities that also have scores ranging between 30.1 and 82.7 on the University of Illinois at Chicago Great Cities Institute's Economic Hardship Index.
2. **Environmental Sustainability** -- Support farmers employing sustainable farming practices by using the least toxic crop protectants reducing the use of synthetic pesticides and fertilizers; utilizing antibiotics only when medically necessary; conserve and regenerate soil and water; protect and enhance wildlife habitat and biodiversity; and reduce on-farm energy consumption and greenhouse gas emissions.
3. **Valued Workforce** - provide safe and healthy working conditions and fair compensation for all food chain workers and producers from production to consumption
4. **Animal Welfare** - provide healthy and humane care for farm animals.
5. **Nutritional** - promote health and well-being by offering generous portions of vegetables, fruit, and whole grains; reducing salt, added sugars, fats, and oils; and by eliminating artificial additives.

BE IT FURTHER RESOLVED, that the following goals are also adopted and implemented as part of Cook County's participation in the Good Food Purchasing Program (GFPP) to address ongoing inequities and issues caused by unequal access to access and resources. Cook County Departments and agencies are tasked with developing multi-year action plans that will address these inequities by pursuing one or more of these possible strategies:

- Encourage businesses to grow food organically and engage in bio-dynamic agriculture, developing incentives for Requests for Proposal reviews and other potential supports during the contracting period; and
- Encourage prospective food vendors to invest in and hire from Priority Communities by: 1) developing bonus scores for Requests for Proposal reviews for prospective vendors demonstrating a track record of hiring and investing in such communities; and 2) assisting prospective vendors in navigating tax incentives and other financial programs designed to increase investment in disadvantaged communities; and
- Encourage conveyance of publicly-owned vacant properties (land and buildings) to local minority owned and/or controlled social enterprises and/or community land trusts for urban agriculture and other food related enterprises in an equitable fashion by setting ownership goals for minority owned and controlled enterprises; developing incentives for Requests for Proposal reviews; exploring possibilities for technical assistance and financial assistance, including tax incentives; and
- Encourage hiring people with arrest and conviction records by developing incentives for Requests for Proposal reviews, exploring options for technical assistance and financial assistance, including tax incentives; and
- Engage local universities, social enterprises and small consulting firms with demonstrated expertise in providing technical assistance to emerging and/or disadvantaged businesses; and

BE IT FURTHER RESOLVED, that the Cook County Department of Public Health (CCDPH) convene a taskforce that includes all relevant Cook County Departments and Agencies involved in the procurement or service contracting of foods, including but not limited to, Offices under the President, the Office of the Chief Judge, the Juvenile Temporary Detention Center, the Office of the Sheriff, the Cook County Health and Hospital System, the Chicago Food Policy Action Council,

the Center for Good Food Purchasing, and other relevant diverse stakeholders,

BE IT FURTHER RESOLVED, that the taskforce recommend flexibility within each of these five value categories and the following steps in support of the purchasing of Good Food and as a framework for guiding values-driven purchasing,

1. Communicate Good Food Purchasing Standards to appropriate suppliers, including distributors and foodservice companies, and ask them to share data that will help the County complete a baseline Good Food Purchasing assessment of food procurement practices within 12 months of the adoption of this resolution.
2. After the baseline assessment has been completed, develop and adopt an multi-year action plan with benchmarks to measure success towards Good Food Purchasing Standards, diversity goals, and programs to support emerging producers and suppliers from Priority Areas and diverse communities including accountability systems with appropriate vendors/distributors to verify sourcing commitments and assess current food procurement practices within 6 months; and
3. After the baseline assessment has been completed, establish supply chain accountability and traceability systems with vendors/distributors to verify sourcing commitments and assess current food procurement practices within 6 months; and
4. To the extent permitted by law, following the multi-year action plan, after the baseline assessment has been completed, incorporate Good Food Purchasing Standards into new procurement requests and contracts within 6 months; and
5. Seek resources as needed to staff and implement the Good Food Purchasing Standards; and

BE IT FURTHER RESOLVED, that the taskforce report its progress to the Health and Hospital Committee within 12 months of the adoption of this resolution, and then report annually on implementation progress; and

BE IT FURTHER RESOLVED, that the taskforce will host an annual public hearing where diverse community stakeholders and residents can ask questions and provide feedback on implementation, including due diligence reporting data to verify compliance, measure progress, and celebrate successes; and

BE IT FURTHER RESOLVED, that the taskforce will engage and encourage municipalities, townships, schools, hospitals and other entities within Cook County to adopt the Good Food Purchasing Policy.

Appendix VIII – Good Food Purchasing Standards and Scoring System





GOOD FOOD PURCHASING STANDARDS AND SCORING SYSTEM OVERVIEW

The Good Food Purchasing Standards are a central component of the Good Food Purchasing Program. The Standards provide institutions with a roadmap for working towards a more sustainable and equitable food system. An institution is expected to meet a baseline in each value category by sourcing a certain percentage of food from producers that reflect each of the five values. The Standards set a basic minimum in each value category, but encourage institutions to earn higher levels of achievement through a flexible, points-based scoring system. Key aspects of the scoring system include:

BASELINE STANDARD

Each of the five value categories has a baseline standard. To become a Good Food Provider, an institution must meet at least the baseline in each of the five values.

CERTIFICATION-BASED

Standards are primarily based off of third-party certifications that have been identified as meaningful and ranked by national experts in each category.

FLEXIBLE, TIERED POINT SYSTEM

Performance is measured using a points-based formula in which points are accumulated based on level of achievement. There are three levels in each category, with higher levels worth more points. Points are awarded for each category individually, allowing institutions to accommodate their priorities and constraints by participating at the baseline in some categories and earning additional points by going above and beyond in other categories.

AGGREGATION OF POINTS AND STAR RATING

Points earned in each category are added together to determine the overall number of points. A star rating is awarded based on the total number of points earned. The minimum score needed to earn One Star and the Good Food Provider seal is five (one point in each category). As points accumulate, higher star ratings are awarded according to the chart below. A participant that earns five or more points only receives the Good Food Provider seal if they meet the baseline standard in each category.

INCREASED COMMITMENT OVER TIME

To maintain the star rating, an institution increases the amount of Good Food purchased each year.

GOOD FOOD PURCHASING AWARD LEVELS

STAR RATING	POINTS
★	5-9
★★	10-14
★★★	15-19
★★★★	20-24
★★★★★	25+



LOCAL ECONOMIES

Support diverse, family and cooperatively owned, small and mid-sized agricultural and food processing operations within the local area or region.

LOCAL ECONOMIES

PURCHASING GOALS

STRATEGIES

- INCREASE SPEND ON LOCAL FOOD

SOURCING TARGETS, BY YEAR

TARGET: YEAR 1

TARGET: YEAR 5

POINTS AWARDED

LEVEL 1 BASELINE

Option 1: Increase Local Food Spend

15% of the total dollars spent annually on food products, with a goal of increasing at least 2% per year, will come from Level 1 local food sources (see page 22 for qualifying sources).

OR

5% of the total dollars spent annually on food products, with a goal of increasing at least 2% per year, will come from Level 3 local food sources.

Option 2: Submit Plan for Baseline Achievement Within 1 Year

If vendor and/or suppliers do not have current capacity to meet local food purchasing goals, the vendor may submit a plan to achieve full compliance at least at the baseline level by end of year one.

To be recognized as a Good Food Provider, an institution at least meets the baseline standard in the Local Economies Category.

Increase Local Food Spend:

25% of the total dollars spent annually on food products will come from Level 1 local food sources by fifth year of participation (see page 22 for qualifying sources).

1

LEVEL 2

Increase Local Food Spend:

15% of the total dollars spent annually on food products, with a goal of increasing at least 2% per year, will come from Level 2 local food sources (see page 22 for qualifying sources).

OR

10% of the total dollars spent annually on food products with a goal of increasing at least 2% per year, will come from Level 3 local food sources.

Increase Local Food Spend:

25% of the total dollars spent annually on food products will come from Level 2 local food sources by fifth year of participation (see page 22 for qualifying sources).

2

LEVEL 3

Increase Local Food Spend

15% of the total dollars spent annually on food products, with a goal of increasing at least 2% per year, will come from Level 3 local food sources (see page 22 for qualifying sources).

Increase Local Food Spend:

25% of the total dollars spent annually on food products will come from Level 3 local food sources by fifth year of participation (see page 22 for qualifying sources).

3

LOCAL ECONOMIES

EXTRA POINTS

EXTRA POINTS

In addition to base points earned in each category, extra points may be earned in each category for institutional policies or purchasing practices that go above and beyond the standards in each value category. An institution may earn a maximum of five bonus points in the Local Economies Extra Points section.

1

At least 1% of food is purchased from small scale and family or cooperatively-owned farms (per the USDA definition of farm size in the most recent USDA Census of Agriculture) and located within 250 miles.

1

At least 5% of food is grown/raised AND processed in the same county as institution.

1

At least 1% of food is purchased directly from farmer-owned businesses.

1

At least 1% of food is purchased from Socially Disadvantaged, Beginning, Limited Resource, Veteran, Women, Minority, or Disabled Farmers/Ranchers.

1

An institution purchases product from suppliers outside 250 mile range, but from small-scale operations and certified by Fairtrade International (FLO) or Small Producer Symbol (SPP).

1-3

DEPENDENT ON
RIGOR OF PROGRAM

Institution develops and implements long-term plan to encourage and invest in value-chain innovation among its suppliers.

Examples of qualifying initiatives:

- Help develop new distribution infrastructure to facilitate working with very small growers, processors or other food businesses.
- Guarantee a certain volume of purchases to small growers prior to each planting cycle.
- Work with suppliers to include alternate ingredients in processed food items that support the Good Food value categories.
- Finance suppliers' certification processes to help them participate in Level 3 certification initiatives.¹

1-3

DEPENDENT ON
RIGOR OF PROGRAM

Institution actively supports or sponsors initiatives that directly promote quality employment or business ownership opportunities for low-income entrepreneurs of color or disadvantaged communities.

Examples of qualifying initiatives:

- Establish a contract, MOU or other formal partnership to purchase food from a community-serving business/organization with a stated mission that includes providing jobs to people with barriers to employment such as those transitioning from homelessness, incarceration, substance abuse or foster care.
- For new facilities development, create a Community Benefits Agreement that considers the workforce, community development and environmental impact of the development.
- Establish a formal hiring policy, which prioritizes hiring local residents with barriers to employment.
- Establish a contract, MOU or other formal partnership to purchase food from a worker-owned cooperative that has a stated mission to serve or is majority-owned by disadvantaged populations.
- Support workforce development in the food industry for disadvantaged or vulnerable populations through scholarships for employees who participate in career pathway training programs or hire new employees directly from a workforce training program.

¹ Food or monetary donations for charitable causes do not count.

LOCAL ECONOMIES

QUALIFYING CRITERIA

The geographic radius of local is defined by region, with agreement by the Center, depending on regional variation in food production patterns. Otherwise, local is defined as:

LEVEL 1

Size

- Produce: Very large scale operations (as per the USDA definition of farm size in the most recent USDA Census of Agriculture)³ (>\$5 million)
- Meat, Poultry, Eggs, Dairy, Seafood & Grocery Items: Very large scale operations (>\$50 million)⁴

AND

Ownership

- Family farm⁵ or cooperatively owned (or owner-operated boats for seafood)

AND

Geographic Radius

- Within 250 miles⁶

LEVEL 2

Size

- Produce: Large scale operations (Between \$1 million and \$5 million)
- Meat, Poultry, Eggs, Dairy, Seafood & Grocery Items: Large scale operations (Between \$20 million and \$50 million)

AND

Ownership

- Family farm or cooperatively owned (or owner-operated boats for seafood)

AND

Geographic Radius

- Within 250 miles⁷

LEVEL 3²

Size

- Produce: Medium scale operations (<\$1 million)
- Meat, Poultry, Eggs, Dairy, Seafood & Grocery Items: Medium scale operations (<\$20 million)

AND

Ownership

- Family farm or cooperatively owned (or owner-operated boats for seafood)

AND

Geographic Radius

- Within 250 miles⁸

² For single and multi-ingredient products, with at least 50% of ingredients sourced from a family or cooperatively-owned medium scale operation within 250 miles, greater credit is given for full supply chain participation at Level 3. Points are weighted as follows:

- 100% credit if source farm meets Level 3 criteria.
- 66% credit if processor or shipper AND distributor, but NOT source farm, meet Level 3 criteria.
- 33% credit if processor or shipper OR distributor, but NOT source farm, meet Level 3 criteria.

³ United States Department of Agriculture (January 2015). "2012 Census of Agriculture: Farm Typology." https://www.agcensus.usda.gov/Publications/2012/Online_Resources/Typology/typology13.pdf.

⁴ Size ranges for meat, poultry, eggs, dairy, seafood, and grocery items are based off of internal analysis of suppliers and align with Real Food Challenge's definitions.

⁵ As defined by the USDA, a majority of the business is owned by the operator and individuals related to the operator. <https://www.ers.usda.gov/topics/farm-economy/farm-household-well-being/glossary.aspx#familyfarm>.

⁶ Note: this radius is 500 miles for meat.

⁷ Note: this radius is 500 miles for meat.

⁸ Note: this radius is 500 miles for meat.



ENVIRONMENTAL SUSTAINABILITY

Source from producers that employ sustainable production systems to reduce or eliminate synthetic pesticides and fertilizers; avoid the use of hormones, routine antibiotics and genetic engineering; conserve and regenerate soil and water; protect and enhance wildlife habitats and biodiversity; and reduce on-farm energy and water consumption, food waste and greenhouse gas emissions. Reduce menu items that have high carbon and water footprints, using strategies such as plant forward menus, which feature smaller portions of animal proteins in a supporting role.

ENVIRONMENTAL SUSTAINABILITY

PURCHASING GOALS

STRATEGIES

- INCREASE ENVIRONMENTALLY SUSTAINABLE FOOD SPEND **OR**
- REDUCE CARBON AND WATER FOOTPRINT

SOURCING TARGETS, BY YEAR

TARGET: YEAR 1

TARGET: YEAR 5

POINTS AWARDED

LEVEL 1 BASELINE

Option 1: Increase Environmentally Sustainable Food Spend

15% of the total dollars spent annually on food products, with a goal of increasing at least 2% per year, will come from Level 1 environmentally sustainable sources (see page 29 for qualifying criteria).

OR

5% of the total dollars spent annually on food products, with a goal of increasing at least 2% per year, will come from Level 3 environmentally sustainable sources (see page 29 for qualifying criteria).

Option 2: Reduce Carbon and Water Footprint

a) Reduce carbon footprint⁹ and water footprint¹⁰ of meat, poultry, and cheese purchases by at least 4% per meal served from baseline year, with an 8% reduction goal within two years, and a 20% reduction goal within five years;^{11, 12}

AND

b) Perform a food waste audit that identifies specific types and quantities of food in waste stream (see Food Loss and Waste Protocol for guidance) and implement at least two source reduction strategies¹³ that address most wasted food items identified in audit. (See Appendix B for a menu of options).¹⁴

Option 3: Submit Plan for Baseline Achievement Within 1 Year:

If vendor and/or suppliers do not have current capacity to meet environmentally sustainable food purchasing goals, the vendor may submit a plan to achieve full compliance at least at the baseline level by end of year one.

ADDITIONAL LEVEL 1 REQUIREMENTS CONTINUED ON PAGE 25

To be recognized as a Good Food Provider, an institution at least meets the baseline standard in the Environmental Sustainability Category.

Option 1: Increase Environmentally Sustainable Food Spend

25% of the total dollars spent annually on food products will come from Level 1 environmentally sustainable sources by fifth year of participation in the Good Food Purchasing Program (see page 29 for qualifying criteria).

Option 2: Reduce Carbon and Water Footprint

a) Reduce carbon and water footprint of meat, poultry, and cheese purchases by at least 20% per meal served from baseline year;

AND

b) Perform a food waste audit that identifies specific types and quantities of food in waste stream (see Food Loss and Waste Protocol for guidance) and implement at least three source reduction strategies that address most wasted food items identified in audit. (See Appendix B for a menu of options).

1

⁹ See next page for conversion factors for carbon footprint.

¹⁰ See next page for conversion factors for water footprint.

¹¹ The baseline year is the year in which institution initiates its meat reduction efforts.

¹² Special calculations of water/carbon for "better meat" will be considered in cases where a credible analysis has been conducted to evaluate the carbon emissions associated with the production of that particular meat source.

¹³ Qualifying food resource recovery strategies will be determined based on adherence to EPA's Food Recovery Hierarchy. See Appendix B for menu of options.

¹⁴ An institution may choose to conduct waste audit at a select number of sample sites.

ENVIRONMENTAL SUSTAINABILITY

PURCHASING GOALS, CONT.

STRATEGIES

- INCREASE ENVIRONMENTALLY SUSTAINABLE FOOD SPEND **OR**
- REDUCE CARBON AND WATER FOOTPRINT

SOURCING TARGETS, BY YEAR

TARGET: YEAR 1

TARGET: YEAR 5

LEVEL 1 BASELINE

ADDITIONAL LEVEL 1 REQUIREMENTS

No seafood purchased should be listed as “Avoid” in the Monterey Bay Aquarium’s most recent Seafood Watch Guide.

No seafood purchased should be listed as “Avoid” in the Monterey Bay Aquarium’s most recent Seafood Watch Guide.

At least 25% of animal products¹⁵ are produced without the routine use of medically important antimicrobial drugs for disease prevention purposes.^{16,17}

At least 50% of animal products are produced without the routine use of medically important antimicrobial drugs for disease prevention purposes.¹⁸

To be recognized as a Good Food Provider, an institution at least meets the baseline standard in the Environmental Sustainability Category.

CONVERSION FACTORS FOR CARBON FOOTPRINT:

Food Product	lb CO2/lb edible
Beef	26.5
Cheese	9.8
Pork	6.9
Poultry	5.1
Fish	3.8
Other Dairy + Eggs	3.3

Source: Heller, M. C. and Keoleian, G. A. (2015), Greenhouse Gas Emission Estimates of U.S. Dietary Choices and Food Loss. Journal of Industrial Ecology, 19: 391–401.

CONVERSION FACTORS FOR WATER FOOTPRINT:

Food Product	Blue + Green gallons/lb edible
Beef	1,590
Pork	475
Cheese	382
Poultry	230
Other Dairy + Eggs	139
Fish	Pending

Source: Mekonnen, M.M. and Hoekstra, A.Y. (2012) A global assessment of the water footprint of farm animal products, Ecosystems, 15(3): 401–415.

¹⁵ Animal product refers to any products derived from an animal, including meat, poultry, eggs and dairy.

¹⁶ In qualifying products, medically important antimicrobial drugs (i.e. those in the same class of antibiotics used in human medicine) may be used for non-routine disease control and treatment purposes only. Antimicrobial use must be third party verified (e.g., Certified Responsible Antibiotic Use (CRAU) chicken, Antimicrobial Stewardship Standards for Pork and Chicken [once 3rd party verified]). Disease control is defined here as the use of antibiotics on an animal that is not sick but where it can be shown that a particular disease or infection is present on the premises at the barn, house, pen, or other level at which the animal is kept. The Center for Good Food Purchasing may consider approval of additional narrowly defined, noncustomary uses upon request.

¹⁷ Addressing antibiotic usage through third party verified certification processes, such as Certified Responsible Antibiotic Use (CRAU) is a separate requirement included in the Environmental Sustainability category. Certification labels that only address responsible antibiotic use are not included as qualifying certifications for environmentally sustainable sources because these labels do not necessarily lead to improved environmental outcomes.

¹⁸ See footnote 16 for definition.

ENVIRONMENTAL SUSTAINABILITY

PURCHASING GOALS, CONT.

STRATEGIES

- INCREASE ENVIRONMENTALLY SUSTAINABLE FOOD SPEND **OR**
- REDUCE CARBON AND WATER FOOTPRINT

SOURCING TARGETS, BY YEAR

TARGET: YEAR 1

TARGET: YEAR 5

POINTS AWARDED

LEVEL 2

Option 1: Increase Environmentally Sustainable Food Spend

15% of the total dollars spent annually on food products, with a goal of increasing at least 2% per year, will come from Level 2 environmentally sustainable sources (see page 29 for qualifying criteria).

OR

10% of the total dollars spent annually on food products, with a goal of increasing at least 2% per year, will come from Level 3 environmentally sustainable sources (see page 29 for qualifying sources).

Option 2: Reduce Carbon and Water Footprint

a) Reduce carbon and water footprint of meat, poultry, and cheese purchases by 5% per meal served from baseline year, with a 10% reduction goal within two years, a 15% reduction in three years and 25% reduction within five years;¹⁹

AND

b) Perform a food waste audit that identifies specific types and quantities of food in waste stream (see Food Loss and Waste Protocol for guidance), and implement at least three source reduction strategies²⁰ that address most wasted food items identified in audit and donate all recoverable food once per month.²¹

LEVEL 2 ADDITIONAL REQUIREMENTS

At least 25% of seafood purchased should be listed as “Best Choice” and no seafood purchased listed as “Avoid” in the Monterey Bay Aquarium’s most recent Seafood Watch Guide.

At least 30% of animal products are produced without the use of antimicrobial drugs for disease prevention purposes.^{22, 23}

Option 1: Increase Environmentally Sustainable Food Spend

25% of the total dollars spent annually on food products will come from Level 1 environmentally sustainable sources by fifth year of participation (see page 29 for qualifying criteria).

Option 2: Reduce Carbon and Water Footprint

a) Reduce carbon and water footprint of meat, poultry, and cheese purchases by at least 20% per meal served from baseline year;

AND

b) Perform a food waste audit that identifies specific types and quantities of food in waste stream (see Food Loss and Waste Protocol for guidance) and implement at least three source reduction strategies that address most wasted food items identified in audit. (See Appendix B for a menu of options).

At least 50% of seafood purchased should be listed as “Best Choice” and no seafood purchased listed as “Avoid” in the Monterey Bay Aquarium’s most recent Seafood Watch Guide.

At least 60% of animal products are produced without the use of antimicrobial drugs for disease prevention purposes.²⁴

¹⁹ The baseline year is the year in which institution initiates its meat reduction efforts.

²⁰ Qualifying food resource recovery strategies will be determined based adherence to EPA’s Food Recovery Hierarchy. See Appendix B for menu of options.

²¹ An institution may choose to conduct waste audit at a select number of sample sites.

²² In qualifying products, antimicrobial drugs (both medically important and otherwise) may be used for disease control and treatment purposes only. Antimicrobial use must be third party verified (e.g., Certified Responsible Antibiotic Use (CRAU) chicken, Antimicrobial Stewardship Standards for Pork and Chicken [once 3rd party verified]). Disease control is defined here as the use of antibiotics on an animal that is not sick but where it can be shown that a particular disease or infection is present on the premises at the barn, house, pen, or other level at which the animal is kept. The Center for Good Food Purchasing may consider approval of additional narrowly defined, noncustomary uses upon request.

²³ Addressing antibiotic usage through third party verified certification processes, such as Certified Responsible Antibiotic Use (CRAU) is a separate requirement included in the Environmental Sustainability category. Certification labels that only address responsible antibiotic use are not included as qualifying certifications for environmentally sustainable sources because these labels do not necessarily lead to improved environmental outcomes.

²⁴ Refer to footnote 22 for definition.

ENVIRONMENTAL SUSTAINABILITY

PURCHASING GOALS, CONT.

STRATEGIES

- INCREASE ENVIRONMENTALLY SUSTAINABLE FOOD SPEND **OR**
- REDUCE CARBON AND WATER FOOTPRINT

SOURCING TARGETS, BY YEAR

TARGET: YEAR 1

TARGET: YEAR 5

POINTS AWARDED

LEVEL 3

15% of the total dollars spent annually on food products, with a goal of increasing at least 2% per year, will come from Level 3 environmentally sustainable sources (see page 29 for qualifying criteria);

25% of the total dollars spent annually on food products will come from Level 3 environmentally sustainable sources by fifth year of participation;

3

AND

AND

Reduce carbon and water footprint of meat, poultry, and cheese purchases by 6% per meal served from baseline year, with a 12% reduction goal within two years and 30% reduction within five years;²⁵

Reduce carbon and water footprint of meat, poultry, and cheese purchases, per meal served by 30% from baseline year;

AND

AND

Perform a food waste audit that identifies specific types and quantities of food in waste stream (see Food Loss and Waste Protocol for guidance), and implement at least three source reduction strategies²⁶ that address most wasted food items identified in audit, donate recoverable food twice per month, and implement one food recycling strategy (e.g. anaerobic digestion or composting).²⁷

Perform a food waste audit that identifies specific types and quantities of food in waste stream (see Food Loss and Waste Protocol for guidance), and implement at least four source reduction strategies that address most wasted food items identified in audit, donate recoverable food once per week, and implement two food recycling strategies.

LEVEL 3 ADDITIONAL REQUIREMENTS

At least 50% of seafood purchased should be listed as “Best Choice” and no seafood purchased listed as “Avoid” in the Monterey Bay Aquarium’s most recent Seafood Watch Guide.

All seafood purchased should be listed as “Best Choice” in the Monterey Bay Aquarium’s most recent Seafood Watch Guide.

At least 50% of animal products are produced without the use of antimicrobial drugs for disease prevention purposes.^{28, 29}

All animal products are produced without the use of antimicrobial drugs for disease prevention purposes.³⁰

²⁵ The baseline year is the year in which institution initiates its meat reduction efforts.

²⁶ Qualifying food resource recovery strategies will be determined based on adherence to EPA’s Food Recovery Hierarchy. See Appendix B for menu of options.

²⁷ An institution may choose to conduct waste audit at a select number of sample sites.

²⁸ Refer to footnote 22.

²⁹ Addressing antibiotic usage through third party verified certification processes, such as Certified Responsible Antibiotic Use (CRAU) is a separate requirement included in the Environmental Sustainability category. Certification labels that only address responsible antibiotic use are not included as qualifying certifications for environmentally sustainable sources because these labels do not necessarily lead to improved environmental outcomes.

³⁰ Refer to footnote 22.

ENVIRONMENTAL SUSTAINABILITY

EXTRA POINTS

EXTRA POINTS

In addition to base points earned in each category, extra points may be earned in each category for institutional policies or purchasing practices that go above and beyond the standards in each value category.

- 1** Institution participates in “Meatless Mondays” campaign or any equivalent meatless day program.
- 1** 100% of disposable flatware, dishes, cups, napkins and other service items are compostable.
- 1** No bottled water is sold or served, and plain or filtered tap water in reusable jugs, bottles or dispensers is available.

ENVIRONMENTAL SUSTAINABILITY

QUALIFYING CRITERIA

LEVEL 1

LEVEL 2

LEVEL 3

FRUITS & VEGETABLES

- Distributor provides grower signed affidavit verifying that produce has been grown without the use of pesticides listed as prohibited for fresh produce by Whole Foods' Responsibly Grown program and all neonicotinoids and affidavit is accompanied by a site visit from institution or community partner; or

Gold certified under ANSI/LEO-4000 the American National Standard for Sustainable Agriculture by Leonardo Academy.

- Protected Harvest certified; or
- Food Alliance certified; or
- Rain Forest Alliance certified; or
- Enrolled in Whole Foods Responsibly Grown program; or
- Platinum certified under ANSI/LEO-4000 the American National Standard for Sustainable Agriculture by Leonardo Academy; or
- USDA Transitional Organic Standard; or
- Sustainably Grown certified; or
- Salmon Safe; or
- LEAF (Linking Environment and Farming)

- USDA Organic; or
- Demeter Certified Biodynamic; or
- Produce grown in a farm or garden at the institution using organic practices

MILK & DAIRY

- AGA Grassfed

- Animal Welfare Approved; or
- Food Alliance Certified

- USDA Organic

POULTRY

- Animal Welfare Approved; or
- Food Alliance Certified

- USDA Organic

EGGS

- Certified Humane Raised and Handled

- Animal Welfare Approved; or
- Food Alliance Certified

- USDA Organic

MEAT

- AGA Grassfed

- Animal Welfare Approved; or
- Food Alliance Certified; or
- Grasslands Alliance Standard

- USDA Organic

FISH (WILD)

- No seafood purchased listed as "Avoid" in the Monterey Bay Aquarium's Seafood Watch Guide

- Fish listed as "Best" choice in Monterey Bay Aquarium's Seafood Watch Guide

- Marine Stewardship Council certified, paired with the MSC Chain of Custody Certification

FISH (FARM-RAISED)

- No seafood purchased listed as "Avoid" in the Monterey Bay Aquarium's Seafood Watch Guide

- Fish listed as "Best" choice in Monterey Bay Aquarium's Seafood Watch Guide³¹

GRAINS

- Pesticide-free

- Food Alliance Certified

- USDA Organic; or
- Demeter Certified Biodynamic

THIRD-PARTY CERTIFICATIONS





VALUED WORKFORCE

Provide safe and healthy working conditions and fair compensation for all food chain workers and producers from production to consumption.

VALUED WORKFORCE

PURCHASING GOALS

STRATEGIES

- INCREASE SPEND ON FAIR FOOD
- SUPPORT LABOR LAW COMPLIANCE ALONG THE SUPPLY CHAIN

SOURCING TARGETS, BY YEAR

TARGET: YEAR 1

TARGET: YEAR 5

POINTS AWARDED

LEVEL 1 BASELINE

Submit Labor Law Compliance Documentation and Take Requested Follow Up Steps with Suppliers

See page 32 for additional details.

AND

Increase Fair Food Spend

5% of the total dollars spent annually on food products, with a goal of increasing at least 2% per year will come from Level 1 fair sources (see page 34 for qualifying sources).

If vendor and/or suppliers do not have current capacity to meet fair food purchasing goals, the vendor may submit a plan to achieve full compliance at least at the baseline level by end of Year 1.

Submit Labor Law Compliance Documentation and Take Requested Follow Up Steps with Suppliers

See page 32 for additional details.

AND

Increase Fair Food Spend

15% of the total dollars spent annually on food products will come from Level 1 fair sources by fifth year of participation (see page 34 for qualifying sources).

1

To be recognized as a Good Food Provider, an institution at least meets the baseline standard in the Valued Workforce Category.

LEVEL 2

Submit Labor Law Compliance Documentation and Take Requested Follow Up Steps with Suppliers

See page 32 for additional details.

AND

Increase Fair Food Spend

5% of the total dollars spent annually on food products, with a goal of increasing at least 2% per year will come from Level 2 fair sources (see page 34 for qualifying sources).

Submit Labor Law Compliance Documentation and Take Requested Follow Up Steps with Suppliers

See page 32 for additional details.

AND

Increase Fair Food Spend

15% of the total dollars spent annually on food products will come from Level 2 fair sources by fifth year of participation (see page 34 for qualifying sources).

2

LEVEL 3

Submit Labor Law Compliance Documentation and Take Requested Follow Up Steps with Suppliers

See page 32 for additional details.

AND

Increase Fair Food Spend

5% of the total dollars spent annually on food products, with a goal of increasing at least 2% per year will come from Level 3 fair sources (see page 34 for qualifying sources).

Submit Labor Law Compliance Documentation and Take Requested Follow Up Steps with Suppliers

See page 32 for additional details.

AND

Increase Fair Food Spend

15% of the total dollars spent annually on food products will come from Level 3 fair sources by fifth year of participation (see page 34 for qualifying sources).

3

VALUED WORKFORCE

PURCHASING GOALS, CONT.

STRATEGIES

- INCREASE SPEND ON FAIR FOOD
- SUPPORT LABOR LAW COMPLIANCE ALONG THE SUPPLY CHAIN

SOURCING TARGETS, BY YEAR

TARGET: YEAR 1

TARGET: YEAR 5

POINTS AWARDED

DETAIL ON LABOR LAW REQUIREMENTS AT ALL LEVELS

Submit Labor Law Compliance Documentation and Take Requested Follow Up Steps with Suppliers

Vendor signs in writing that vendor and all suppliers respect the freedom of association of farmers, ranchers, and fisherfolk and that vendor and all suppliers³² comply with domestic labor law (including state and local) in countries where they produce goods and services, as well as the core standards of the International Labour Organization (ILO):

- (1) Freedom of association and the right to collective bargaining.
- (2) Elimination of all forms of forced or compulsory labor.
- (3) Abolition of child labor.
- (4) Elimination of discrimination with respect to employment or occupation.

AND

If vendor and/or suppliers are found to have health & safety and/or wage & hour violations within the past three years, purchaser requests information from that supplier about steps taken to mitigate past violations and prevent future violations, such as worker education and training. The institution may reserve the right to cancel the contract with a vendor with serious, willful, repeated, and/or pervasive labor violations and/or require its vendor to cancel its contract with the supplier with serious, willful, repeated, and/or pervasive violations over the next year after the letter is sent.

Submit Labor Law Compliance Documentation and Take Requested Follow Up Steps with Suppliers

Vendor signs in writing that vendor and all suppliers respect the freedom of association of farmers, ranchers, and fisherfolk and comply with domestic labor law (including state and local) in countries where they produce goods and services, as well as the core ILO standards.

AND

If vendor and/or suppliers are found to have health & safety and/or wage & hour violations within the past three years, purchaser requests information from that supplier about steps taken to mitigate past violations and prevent future violations, such as worker education and training. The institution may reserve the right to cancel the contract with a vendor with serious, willful, repeated, and/or pervasive labor violations and/or require its vendor to cancel its contract with the supplier with serious, willful, repeated, and/or pervasive violations over the next year after the letter is sent.

³² Vendor refers to the distributor with whom the institution or its food service management company has a direct contract. Supplier refers to all companies in the vendor's supply chain from whom product is sourced to be provided to the institution. A single product may have more than one supplier, including grower, shipper, processor, and/or wholesaler.

VALUED WORKFORCE

EXTRA POINTS

EXTRA POINTS

In addition to base points earned in each category, extra points may be earned in each category for institutional policies or purchasing practices that go above and beyond the standards in each value category.

- 2** Institution establishes an anonymous reporting system for workers to report violations with a protection for workers from retaliation.
- 1** Institution has adopted a “living wage” policy to ensure direct employees are paid non-poverty wages.
- 1** Institution’s food service contractor meets Level 3 Valued Workforce criteria.
- 2** An institution or vendor has a Labor Peace policy or agreement

VALUED WORKFORCE

QUALIFYING CRITERIA

LEVEL 1

Vendor and Suppliers

Have a social responsibility policy, which includes:

- (1) union or non-poverty wages;
- (2) respect for freedom of association and collective bargaining;
- (3) safe and healthy working conditions;
- (4) proactive policy on preventing sexual harassment and assault;
- (5) prohibition of child labor, as defined by the International Labour Organization (ILO)³⁵ and at least one additional employment benefit such as:
- (6) employer-paid health insurance
- (7) paid sick days;
- (8) profit-sharing with all employees;

OR

Vendor and Suppliers

Post information about their participation in the Good Food Purchasing Program in workplaces and in the primary languages spoken by the employees;

OR

Partner with local trade union and/or independent, representative worker organizations to conduct periodic mandatory, accessible, in-depth worker education training at the worksite and on the clock about their rights and ensure they know what their company has committed to as a vendor of a Good Food Purchasing Program participant;

OR

- Are certified by Fair for Life; or
- Are certified by Fairtrade America (Fairtrade International FLO); or
- Are certified by Fairtrade USA

LEVEL 2

Vendor and Supplier

- Are Food Justice-Certified by the Agricultural Justice Project; or
- Are certified by the Equitable Food Initiative

LEVEL 3^{33, 34}

Vendor and Supplier

- Have a union contract with their employees³⁶; or
- Are a worker cooperative³⁷

THIRD-PARTY CERTIFICATIONS



Food items from suppliers that meet any of the following criteria will be disqualified from being counted for points in all value categories:

- **Use of slave or forced labor;**
- **Pattern of serious, willful, repeated, and/or pervasive labor violations over the last three years;**
- **Use of child labor³⁸**

³³ Greater credit is given for full supply chain participation at Level 3. An institution receives 3 points for every 5% increment of product sourced from Level 3 farms, and 3 points for every 15% increment of product sourced from Level 3 processors or distributors (percentages determined related to availability of Level 3 product in sectors of the supply chain). Points are weighted as follows:

- 100% credit if source farm, AND processor or shipper, AND distributor meet Level 3 criteria.
- 66% credit if two of three companies meet Level 3 criteria.
- 33% credit if one of three companies meets Level 3 criteria.

³⁴ Criteria used to identify voluntary third party certification programs at Level 3 include: adherence to all ILO Fundamental Principles and Rights at Work; a fair wage that at a minimum reaches the prevailing industry wage and charts progress toward a living wage; safe and healthy workplaces for workers; inclusion of independent worker organizations at all stages of standard-setting, monitoring and enforcement, and remediation; a confidential complaint reporting and resolution mechanism with a strictly enforced no-retaliation policy; mandatory worker rights training on the clock, implemented with independent worker organization; regular announced and unannounced audits by well-trained auditors that include secure interviews with a broad swath of workers, and findings that are made available to workers; and a focus on enforcement, with binding legal agreements that ensure real consequence for non-compliance and clear, time-bound plans to remedy violations. If the Center determines that a supplier is not compliant with the standards established by the third-party certification program, the supplier will not receive credit for their participation in the certification program.

³⁵ <http://ilo.org/ipec/facts/lang-en/index.htm>.

³⁶ Unions cannot be controlled or backed by government or the employer

³⁷ As defined by United States Federation of Worker Cooperatives: Worker cooperatives are business entities that are owned and controlled by their members, the people who work in them. All cooperatives operate in accordance with the [Cooperative Principles and Values](#). The two central characteristics of worker cooperatives are: (1) worker-members invest in and own the business together, and it distributes surplus to them and (2) decision-making is democratic, adhering to the general principle of one member-one vote.

³⁸ Federal and/or state law defines child labor for the supplier's industry and location. When federal and state rules are different, the rules that provide the most protection apply. For international products, child labor is defined by the [ILO standard](#).



ANIMAL WELFARE

Source from producers that provide healthy and humane conditions for farm animals.

ANIMAL WELFARE

PURCHASING GOALS

STRATEGIES

- INCREASE HIGH ANIMAL WELFARE FOOD SPEND **OR**
- REDUCE TOTAL VOLUME OF ANIMAL PRODUCTS PURCHASED

SOURCING TARGETS, BY YEAR

TARGET: YEAR 1

TARGET: YEAR 5

POINTS AWARDED

LEVEL 1 BASELINE

Option 1: Increase High Animal Welfare Food Spend

15% of the total dollars spent annually on egg, dairy, and meat products will come from products that meet Level 1 animal welfare requirements (see page 39 for qualifying criteria).

OR

5% of the total dollars spent annually on egg, dairy, and meat products will come from products that meet Level 3 animal welfare requirements (see page 39 for qualifying criteria).

Option 2: Reduce Total Volume of Animal Products Purchased

Replace 15% of the total volume of animal products purchased with plant-based protein.

Option 1: Increase High Animal Welfare Food Spend

25% of the total dollars spent annually on egg, dairy, and meat products will come from products that meet at least Level 1 requirements (see page 39 for qualifying criteria).

Option 2: Reduce Total Volume of Animal Products Purchased

Replace 25% of the total volume of animal products purchased with plant-based protein.

1

To be recognized as a Good Food Provider, an institution at least meets the baseline standard in the Animal Welfare Category.

LEVEL 2

Option 1: Increase High Animal Welfare Food Spend

15% of the total dollars spent annually on egg, dairy, and meat products will come from products that meet at least Level 2 requirements (see page 39 for qualifying criteria).

OR

10% of the total dollars spent annually on egg, dairy, and meat products will come from products that meet Level 3 animal welfare requirements (see page 39 for qualifying criteria).

Option 2: Reduce Total Volume of Animal Products Purchased

Replace 25% of the total volume of animal products purchased with plant-based protein.

Option 1: Increase High Animal Welfare Food Spend

35% of the total dollars spent annually on egg, dairy, and meat products will come from products that meet at least Level 2 requirements (see page 39 for qualifying criteria).

Option 2: Reduce Total Volume of Animal Products Purchased

Replace 35% of the total volume of animal products purchased with plant-based protein.

2

ANIMAL WELFARE

PURCHASING GOALS, CONT.

STRATEGIES

- INCREASE HIGH ANIMAL WELFARE FOOD SPEND **OR**
- REDUCE TOTAL VOLUME OF ANIMAL PRODUCTS PURCHASED

SOURCING TARGETS, BY YEAR

TARGET: YEAR 1

TARGET: YEAR 5

POINTS AWARDED

LEVEL 3

Option 1: Increase High Animal Welfare Food Spend

15% of the total dollars spent annually on egg, dairy, and meat products will come from products that meet at least Level 3 requirements (see page 39 for qualifying criteria).

Option 2: Reduce Total Volume of Animal Products Purchased

Replace 35% of the total *volume* of animal products purchased with plant-based protein.

Option 1: Increase High Animal Welfare Food Spend

45% of the total dollars spent annually on egg, dairy, and meat products will come from products that meet at least Level 3 requirements (see page 39 for qualifying criteria).

Option 2: Reduce Total Volume of Animal Products Purchased

Replace 40% of the total *volume* of animal products purchased with plant-based protein.

3

ANIMAL WELFARE

EXTRA POINTS

EXTRA POINTS

In addition to base points earned in each category, extra points may be earned in each category for institutional policies or purchasing practices that go above and beyond the standards in each value category.

- 2** Institution encourages plant-based diets by offering only vegan options.
- 1** Institution encourages plant-based diets by offering only vegetarian options.
- 1** 50% or more annual average of total cost of milk, egg and meat product purchases come from higher-welfare sources (Level 1 or above).

ANIMAL WELFARE

QUALIFYING CRITERIA

LEVEL 1

LEVEL 2

LEVEL 3

DAIRY

- Certified Humane; or
- USDA Organic³⁹

- PCO 100% Grassfed

- Animal Welfare Approved

EGGS⁴⁰

- Certified Humane Cage Free; or
- GAP Step 1, 2; or
- USDA Organic⁴¹

- American Humane Certified Pasture Raised⁴²; or
- Certified Humane Free Range; or
- GAP Step 3

- Animal Welfare Approved; or
- Certified Humane Pasture Raised; or
- GAP Step 4, 5, 5+

POULTRY

- Certified Humane; or
- GAP⁴³ Step 2, 3; or
- USDA Organic⁴⁴

- Certified Humane Free Range⁴⁵

- Animal Welfare Approved; or
- GAP Step 4, 5, 5+

BEEF

- Approved American Grassfed Association Producer; or
- Certified Humane; or
- GAP Step 1, 2; or
- USDA Organic⁴⁶

- PCO 100% Grassfed

- Animal Welfare Approved; or
- Certified Grassfed by A Greener World; or
- GAP Step 4, 5, 5+

PORK

- Certified Humane; or
- GAP Step 1, 2; or
- USDA Organic⁴⁷

- Gap Step 3

- Animal Welfare Approved; or
- GAP Step 4, 5, 5+

FISH⁴⁸

THIRD-PARTY CERTIFICATIONS



³⁹ USDA Certified Organic will qualify for Level 2 if proposed animal welfare requirements are adopted.

⁴⁰ AHA cage-free standards were excluded because AHA's points-based system allows egg facilities to pass an audit (at 85%) without meeting a number of basic welfare standards.

⁴¹ USDA Certified Organic will qualify for Level 2 if proposed animal welfare requirements are adopted.

⁴² Because American Humane Certified does not have a set of "Core Criteria" that all certified producers must meet, full audit results must be submitted to the Center to verify that the farm meets all Core Criteria for a product to meet Level 2.

⁴³ GAP Step 1 may be added to Level 1 upon the adoption of requirements for enrichments and for slower-growing chicken strains at Step 1.

⁴⁴ USDA Certified Organic will qualify for Level 2 if proposed animal welfare requirements are adopted.

⁴⁵ Certified Humane Free Range, despite being pasture-based, is in Level 2 because unlike those in Level 3, it does not require slower-growth genetics.

⁴⁶ USDA Certified Organic will qualify for Level 2 if proposed animal welfare requirements are adopted.

⁴⁷ USDA Certified Organic will qualify for Level 2 if proposed animal welfare requirements are adopted.

⁴⁸ Standards for farm raised fish are in development and will be added to the Good Food Purchasing Standards as soon as possible.



NUTRITION

Promote health and well-being by offering generous portions of vegetables, fruit, whole grains, and minimally processed foods, while reducing salt, added sugars, saturated fats, and red meat consumption and eliminating artificial additives.

NUTRITION

PURCHASING GOALS

STRATEGIES

POINTS AWARDED

HIGH PRIORITY

- IMPLEMENT HEALTHFUL PRACTICES IN PROCUREMENT, FOOD PREPARATION, AND FOOD SERVICE ENVIRONMENT

2 CHECKS

Items with High Priority designation are worth two checks per item met

HEALTHY PROCUREMENT

- ☐ Increase the amount of whole or minimally processed foods purchased by 5% from baseline year, with a 25% increase goal within 5 years.⁴⁹
- ☐ If meat is offered, reduce purchase of red and processed meat by 5% from baseline year, with a 25% reduction goal within 5 years.^{50, 51}
- ☐ Fruits, vegetables, and whole grains account for at least 50% of total food purchases by volume.⁵²
- ☐ All individual food items contain ≤ 480 mg sodium per serving.⁵³ Purchase “low sodium” (≤ 140 mg sodium per serving) whenever possible.
- ☐ Added sugars (including natural and artificial sweeteners) in purchased food items should be no more than 10% of Daily Value per serving (DV is 50g). Or, commit to implementing an added sugar reduction plan in overall food and beverage purchases.

HEALTHY FOOD SERVICE ENVIRONMENT

- ☐ Healthy beverages account for 100% of beverage options offered, and diet drinks containing artificial sweeteners are eliminated. If healthy beverages account for at least 50% of beverage options offered, one check will be earned.⁵⁴
- ☐ Offer free drinking water at all meals, preferably cold tap water in at least a 4 oz. cup.
- ☐ Offer plant-based main dishes at each meal service.⁵⁵

HEALTH EQUITY

- ☐ Institution actively supports or sponsors initiatives that directly expand access to healthy food for low-income residents or communities of color.⁵⁶ Examples of qualifying initiatives:
 - Support at least one neighborhood-based community food project that expands access to healthy food for low-income residents such as a procurement agreement with a corner store that carries healthy food in a low-income census tract, or a low-cost Community Supported Agriculture program dedicated to serving low-income families, or a farmer’s market located in a low-income census tract that accepts EBT.

⁴⁹ See Appendix C for definitions for whole/minimally processed, processed, and ultraprocessed (Source: San Diego County Department of Public Health Eat Well Standards).

⁵⁰ Processed meats include any meat preserved by curing, salting, smoking, or have other chemical preservation additives. If processed meats are offered, recommend using only products with no more than 480mg of sodium per 2 oz.

⁵¹ One strategy to reduce red and processed meat purchases is to limit portion sizes based on current US Dietary Guidelines. Average per-meal amount for meat, poultry and eggs for a 2000 calorie diet is 1.9 oz. (The range for a 1000-2200 calorie diet is .7-2 oz. per meal). See the [USDA Food Patterns: Healthy U.S.-Style Eating Pattern](#) for more information.

⁵² Grain-based foods are considered whole grain when the first ingredient listed on the ingredient list is a whole grain. Whole grain ingredients include brown rice, buckwheat, bulgur, millet, oatmeal, quinoa, rolled oats, whole-grain barley, whole-grain corn, whole-grain sorghum, whole-grain triticale, whole oats, whole rye, whole wheat, and wild rice. With the exception of the following foods:

⁵³ **Sodium Standards for Purchased Food:**

- Canned and frozen seafood: ≤ 290 mg sodium per serving;
- Canned and frozen poultry: ≤ 290 mg sodium per serving;
- Sliced sandwich bread: ≤ 180 mg sodium per serving;
- Baked goods (e.g. dinner rolls, muffins, bagels, tortillas): ≤ 290 mg sodium per serving;
- Cereal: ≤ 215 mg sodium per serving;
- Canned or frozen vegetables: ≤ 290 mg sodium per serving;
- Recommend “reduced” sodium (per FDA definition) sauce and other condiments;
- Recommend purchasing cheese: ≤ 215 mg sodium per serving.

⁵⁴ Health Care Without Harm “Healthy Beverage Defined: Water (filtered tap, unsweetened, seltzer or infused); 100 percent fruit juice (optimal 4 oz. serving); 100% vegetable juice (optimal sodium less than 140 mg); Milk (unflavored); Non-dairy milk alternatives (plain, unsweetened); Teas and Coffee (unsweetened with only naturally occurring caffeine).

⁵⁵ To the best possible ability, beverages should be dispensed by tap or fountain AND reusable beverage containers should be encouraged. Recommend plant-based main dishes to include fruits, vegetables, beans and/or legumes.

⁵⁶ Food or monetary donations for charitable causes do not count.

NUTRITION

PURCHASING GOALS

STRATEGIES

- IMPLEMENT HEALTHFUL PRACTICES IN PROCUREMENT, FOOD PREPARATION, AND FOOD SERVICE ENVIRONMENT

POINTS AWARDED

PRIORITY

HEALTHY PROCUREMENT

- ☐ All juice purchased is 100% fruit juice with no added sweeteners and vegetable juice is Low Sodium as per FDA definitions. All 100% fruit and vegetable juice single serving containers are <12 ounces for adults and children aged 7-18, and <6 oz. for children aged 1-6.⁵⁷
- ☐ If dairy products are offered, purchase Fat-Free, Low-Fat or reduced fat dairy products, with no added sweeteners (including natural and artificial sweeteners).⁵⁸
- ☐ All pre-packaged food has zero grams trans fat per serving and does not list partially hydrogenated oils on the ingredients list (as labeled).
- ☐ At least 50% of grain products purchased are whole grain rich.⁵⁹
- ☐ Offer at least one salad dressing option that is a low-sodium, low-calorie, low-fat creamy salad dressing.⁶⁰ Offer olive oil and vinegar (e.g., balsamic, red wine) at each meal service.

HEALTHY FOOD PREPARATION

- ☐ Eliminate the use of hydrogenated and partially hydrogenated oils for cooking and baking. Eliminate the use of deep frying and eliminate use of frozen or prepared items that are deep fried upon purchase.
- ☐ Prioritize the preparation of all vegetables and protein, including fish, poultry, meat, or meat alternatives in a way that utilizes vegetable-based oils or reduces added fat (broiling, grilling, baking, poaching, roasting, or steaming).

HEALTHY FOOD SERVICE ENVIRONMENT

- ☐ If applicable, combination meals that serve an entrée, side option, and beverage offer water as a beverage alternative⁶¹ AND offer fresh fruit or a non-fried vegetable prepared without fat or oil as a side option.
- ☐ Adopt one or more product placement strategies such as:
 - Prominently feature fruit and/or non-fried vegetables in high-visibility locations.
 - Display healthy beverages in eye level sections of beverage cases (if applicable).
 - Remove candy bars, cookies, chips and beverages with added sugars (such as soda, sports and energy drinks) from checkout register areas/point-of-purchase (if applicable).
- ☐ Healthy food and beverage items are priced competitively with non-healthy alternatives.
- ☐ Adopt one or more marketing/promotion/signage strategies, such as:
 - Highlight fruit with no-added sweeteners and non-fried vegetable offerings with signage.

1

CHECK

Items with Priority designation are worth one check per item met

⁵⁷ Low Sodium is 140 mg or less per RACC.

⁵⁸ Fat-Free is 0.5g or less per RACC; Low-Fat is 3 g or less per RACC and per 50g if RACC is small (<30g); Reduced fat is 25% less fat per RACC when compared to the original food; Low Sodium is 140 mg or less per RACC and per 50g if RACC is small (<30g).

⁵⁹ Grain-based foods are considered whole grain when the first ingredient listed on the ingredient list is a whole grain. Whole grain ingredients include brown rice, buckwheat, bulgur, millet, oatmeal, quinoa, rolled oats, whole-grain barley, whole-grain corn, whole-grain sorghum, whole-grain triticale, whole oats, whole rye, whole wheat, and wild rice; 3 grams or more of fiber/serving.

⁶⁰ Low-Fat is 3 g or less per RACC and per 50g if RACC is small (<30g); Low Sodium is 140 mg or less per RACC and per 50g if RACC is small (<30g); Low Calorie is 40 calories or less per RACC and per 50g if RACC is small (<30g).

⁶¹ A cup/glass of chilled tap water is prioritized and water in recyclable bottle is a secondary substitute to be avoided if possible for environmental considerations.

NUTRITION

EXTRA POINTS & SCORING TARGETS

EXTRA POINTS

In addition to base points earned in each category, extra points may be earned in each category for institutional policies or purchasing practices that go above and beyond the standards in each value category. An institution may earn a maximum of five bonus points in the Nutrition Extra Points section.

- 1** **MENU LABELING**
Menu lists the nutritional information for each item using the federal menu labeling requirements under the Patient Protection and Affordable Care Act of 2010 as a guide.
- 1** **PORTION CONTROL**
Adopt one or more portion control strategies, if applicable. (e.g. Utilize 10" or smaller plates for all meals; make available reduced-size portions of at least 25% of menu items offered; offer reduced-size portions at a lower price than regular sized portions, eliminate trays from lines).⁶²
- 1** **CULTURALLY APPROPRIATE MENUS**
Offer menu items that are culturally appropriate for institution's demographic composition. Institution should submit menus with ingredient lists for culturally appropriate items.
- 1** **NUTRITION & FOOD SYSTEMS EDUCATION**
For K-12 institutions: Institution implements nutrition education programming. Examples of qualifying initiatives include:
 - Interactive/educational garden program
 - District-wide required nutrition curriculum
 - Farm/processing site visits to regional producers
- 1** **WORKSITE WELLNESS**
Develop and implement a worksite wellness program for employees and/or patrons that includes nutrition education.
- 1** **HEALTHY VENDING**
Adopt a healthy vending machine policy for machines at all locations, using the Federal Food Service Guidelines or a higher standard.⁶³

PERCENTAGE OF CHECKLIST ITEMS MET

SCORING TARGET

POINTS AWARDED

51 - 64.9%

LEVEL 1

1

65 - 79.9%

LEVEL 2

2

80 - 100%

LEVEL 3

3

UP TO **6** EXTRA POINTS

⁶² Reduced-sized portions are at least 1/3 smaller than the full-size item and are offered in addition to the full-size versions.

⁶³ Food Service Guidelines for Federal Facilities:

https://www.cdc.gov/obesity/downloads/guidelines_for_federal_concessions_and_vending_operations.pdf, pages 13-14.



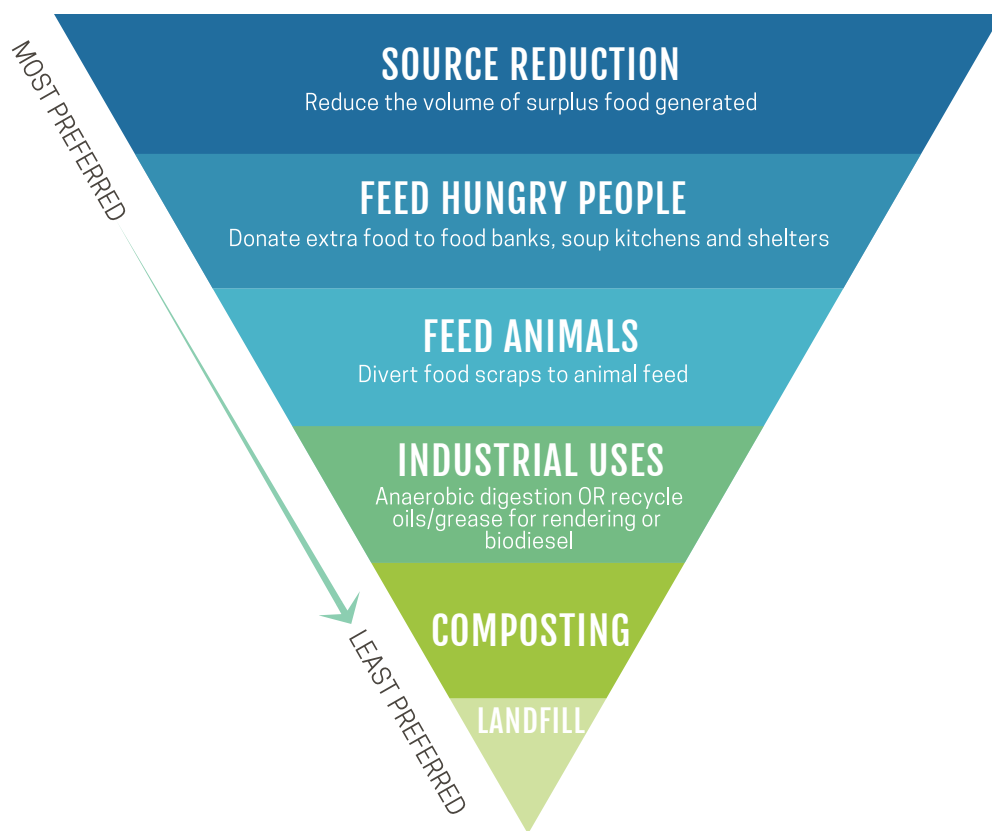
APPENDICES

APPENDIX A: EPA FOOD RECOVERY HIERARCHY: IDENTIFYING AND PRIORITIZING STRATEGIES TO REDUCE WASTED FOOD



The EPA has developed the Food Recovery Hierarchy to help prioritize actions that organizations can take to prevent wasted food. Reduction/diversion points include:

1. Source Reduction – reduce the amount of surplus food generated
2. Recovery: Feed Hungry People – donate extra food to food banks, soup kitchens, shelters
3. Recycling:
 - Feed Animals – divert food scraps to animal feed
 - Industrial Uses – anaerobic digestion (send food to anaerobic digester) OR recycle oils/grease (for rendering or biodiesel)
 - Composting



According to the EPA, “each tier of the Food Recovery Hierarchy focuses on different management strategies for wasted food. The top levels of the hierarchy are the best ways to prevent and divert wasted food because they create the most benefits for the environment, society and the economy.”

Good Food Providers that incorporate waste reduction strategies into their food service operations are encouraged to follow the EPA’s Food Recovery Hierarchy and prioritize strategies at the top levels of the hierarchy.

An important first step for an institution is to perform a waste audit and then develop waste reduction strategies that address the most wasted food items identified in audit.

APPENDIX A: SUGGESTED FOOD RECOVERY STRATEGIES

The list below provides a menu of options that institutions can take to prevent and divert wasted food. This list is by no means exhaustive. Some strategies may not apply to or be feasible for all institution types. More ideas can be found on the EPA's Food Recovery Hierarchy website.

SOURCE REDUCTION⁶⁴

- Purchase imperfect produce
- Staff training on food waste reduction
- Daily log of kitchen food waste⁶⁵
- Reduce batch sizes
- Cook-to-order instead of bulk-cooking at end of day
- Set up share tables
- "Offer vs serve"
- Replace buffet with cook-to-order line
- Finish preparation at the line
- Recess before lunch
- Provide another beverage choice (e.g. water)
- Extend lunch periods to 30 minutes
- Slice fruit/vegetables
- Catchy names for fruits/vegetables
- Marinate meats
- Healthy foods within reach
- Train staff on knife skills
- Use maximum amount of food parts (carrot greens and potato skins)
- Reconstitute wilted veggies
- Freeze surplus fruits & veggies
- Use leftovers
- Eliminate garnishes that typically don't get eaten
- Storage techniques for different foods
- See-through storage containers
- Smaller serving containers at end of day
- Trayless dining

RECOVERY⁶⁶ FEED HUNGRY PEOPLE

- Deliver unused food to local pantry
- Supplement Power Pack program with unused food that is collected
- Pop Up Food Pantry
- Partner with sister school & donate surplus food to families in need

RECYCLING FEED ANIMALS, INDUSTRIAL USES, COMPOSTING

- Provide organic waste to animal farmers as feed
- Send food scraps to anaerobic digester
- Recycle waste vegetable oil to be used as biofuel
- Community or on-site composting of organic waste

⁶⁴ This list is not exhaustive and options are not exclusive to the listed institution type. More ideas can be found at <https://www.epa.gov/sustainable-management-food/food-loss-prevention-options-grade-schools-manufacturers-restaurant>

⁶⁵ LeanPath is one tool institutions can use to monitor kitchen waste. It may be cost prohibitive for some, but a manual log or less costly tool could also be used to monitor kitchen waste. <http://www.leanpath.com>

⁶⁶ From Food Bus: <http://foodbus.org/toolkit/>

APPENDIX B: LEVELS OF PROCESSING – DEFINITIONS

PROCESSING CATEGORY

DEFINITION

EXAMPLES

UNPROCESSED AND MINIMALLY PROCESSED FOODS AND BEVERAGES

Unprocessed and minimally processed foods and beverages include single-ingredient foods or beverages, which have undergone no or slight alterations after separation from nature, such as cleaning, removal of unwanted or inedible parts, fractioning, grinding, roasting, boiling, freezing, drying, fermentation, or pasteurization. These do not include any added oils, fats, sugar, salt or other substances, but may include vitamins and minerals typically to replace those lost during processing. Simple combinations of two or more unprocessed or minimally processed foods, such as granola made from cereals, mixtures of frozen vegetables, and unsalted, unsweetened, dried fruit and nut mixtures, remain in this group. As a general rule, additives are rarely present in food items in this group.^{68, 69, 70, 71, 72}

Examples include, but are not limited to fresh, chilled, frozen, vacuum- packed fruits, vegetables, including those with antioxidants, roots, and tubers; cereal grains and flours made with these grains; cereal products, such as plain oatmeal; fresh or dry pasta or noodles (made from flour with the addition only of water); fresh, frozen and dried beans and other pulses (legumes); dried fruits and 100% unsweetened fruit juices; fresh or dried mushrooms; unsalted nuts and seeds; fresh, dried, chilled, frozen meats, poultry and fish; fresh and pasteurized milk, ultra-pasteurized milk with added stabilizers, fermented milk such as plain yogurt; spices such as pepper, cloves, and cinnamon; herbs such as fresh or dry thyme, mint, and cilantro; eggs; teas, coffee, herb infusions, tap water, bottled spring water.⁷³

MODERATELY PROCESSED FOODS AND BEVERAGES

Moderately processed foods and beverages are simple products manufactured by industry typically with few ingredients including unprocessed or minimally processed foods and salt, sugar, oils, fats and other substances commonly used as culinary ingredients.^{74, 75, 76, 77} Additives are sometimes added to foods in this group.⁷⁸

Examples include, but are not limited to breads; cheese; sweetened fruits and fruits in syrup with added anti-oxidants; dried salted meats with added preservatives; canned foods preserved in salt or oil; cereal products with tocopherols (Vitamin E), such as instant oatmeal with sugar and cinnamon or whole wheat kernels combined with flaxseed, salt, and barley malt; tofu, tempeh, and certain kinds of bean and vegetable burgers; and multi-ingredient foods and beverages manufactured and packaged by industry that contain no ingredients only used in ultra-processed products.

⁶⁷ Courtesy of San Diego County Department of Public Health

⁶⁸ Monteiro C.A., Cannon G., Levy R.B. et al. NOVA. The star shines bright. [Food classification. Public health] *World Nutrition*. January-March 2016, 7, 1-3, 28-38.

⁶⁹ Food and Agriculture Organization of the United Nations (2015) Guidelines on the collection of information on food processing through food consumption surveys. Rome: FAO.

⁷⁰ Monteiro CA, Cannon G, Levy RB, Claro RM, Moubarac J-C. (2015). Ultra-processing and a new classification of foods. In: Neff R (ed) *Introduction to the US food system: Public health, environment, and equity*. Johns Hopkins Center for a Livable Future, San Francisco, CA: Jossey-Bass, 2015.

⁷¹ Poti, J. M., Mendez, M. A., Wen Ng, S., & Popkin, B. M. (2015). Is the degree of food processing and convenience linked with the nutritional quality of foods purchased by US households? *American Journal of Clinical Nutrition*. doi:10.3945/ajcn.114.100925

⁷² Classes of additives that may infrequently be added to foods and beverages in this category include nutrient supplements, stabilizers (in fluid milk or yogurt only), and anti-oxidants or antimicrobial agents to preserve original properties or prevent microorganism proliferation.

⁷³ Monteiro, C.A., Levy, R.B., Claro, R.M., Castro, I.R.R.D., & Cannon, G. (2010). A new classification of foods based on the extent and purpose of their processing. *Cadernos de saude publica*, 26(11), 2039-2049.

⁷⁴ Monteiro C.A., Cannon G., Levy R.B. et al. NOVA. The star shines bright. [Food classification. Public health] *World Nutrition*. January-March 2016, 7, 1-3, 28-38.

⁷⁵ Food and Agriculture Organization of the United Nations (2015) Guidelines on the collection of information on food processing through food consumption surveys. Rome: FAO.

⁷⁶ Monteiro CA, Cannon G, Levy RB, Claro RM, Moubarac J-C. (2015). Ultra-processing and a new classification of foods. In: Neff R (ed) *Introduction to the US food system: Public health, environment, and equity*. Johns Hopkins Center for a Livable Future, San Francisco, CA: Jossey-Bass, 2015.

⁷⁷ Poti, J. M., Mendez, M. A., Wen Ng, S., & Popkin, B. M. (2015). Is the degree of food processing and convenience linked with the nutritional quality of foods purchased by US households? *American Journal of Clinical Nutrition*. doi:10.3945/ajcn.114.100925

⁷⁸ Classes of additives sometimes added to foods and beverages in this category include nutrient supplements, curing and pickling agents, leaving agents (in simple breads), enzymes (in cheese), stabilizers (in fluid milk or yogurt only), and anti-oxidants or antimicrobial agents to preserve original properties or prevent microorganism proliferation or stabilizers.

APPENDIX B: LEVELS OF PROCESSING – DEFINITIONS

PROCESSING CATEGORY	DEFINITION	EXAMPLES
ULTRA-PROCESSED FOOD AND BEVERAGE PRODUCTS	Ultra-processed food and beverage products are industrial formulations typically with many ingredients including salt, sugar, oils and fats, but also substances not commonly used in domestic cooking and additives whose purpose is to imitate sensorial qualities of unprocessed or minimally processed foods and culinary preparations of these foods. Minimally processed foods are a small proportion of or are even absent from ultra-processed products. ^{79, 80, 81, 82}	Examples include, but are not limited to industrially manufactured sports drinks; regular and diet sodas; flavored milks; energy drinks; meal replacement or dietary supplement drinks or foods; cereal products with tocopherols (Vitamin E) and an assortment of additives, such as FD&C Blue No. 1 and 2, caramel color; gelatin; high fructose corn syrup; dextrose or hydrogenated vegetable oil; sweet and/or savory snacks; ice cream; cakes and cake mixes; pastries; candies; chocolate bars; energy bars; granola bars; snack chips and mixes; packaged desserts; grain-based desserts and breads; margarine; condiments; instant sauces and soups; hot dogs; sausages; luncheon meats; chicken patties and nuggets; breaded fish and sticks; frozen and packaged meals; prepacked pizza; fast food; and other foods with ingredients not usually sold to consumers for use in freshly prepared foods.
CULINARY INGREDIENTS	Culinary ingredients are substances obtained from unprocessed or minimally processed foods, or nature, and commonly used to season and cook unprocessed or minimally processed foods in the creation of freshly prepared dishes. Items in this group are rarely consumed alone. Combinations of two or more culinary ingredients, such as oil and vinegar, remain in this group. As a general rule, additives are rarely present in these foods and beverages. ^{83, 84, 85, 86}	Examples include, but are not limited to butter, lard, and vegetable oils; milk, cream; sugar and molasses obtained from cane or beet; honey extracted from combs and syrup from maple trees; salt and iodized salt; starches; vegetable oils with added antioxidants; and vinegar with added preservatives.
FRESHLY PREPARED FOODS AND BEVERAGES	Freshly prepared foods and beverages are handmade preparations composed of unprocessed or minimally processed foods and culinary ingredients. ⁸⁷	Examples include, but are not limited to any scratch prepared foods and beverages made with unprocessed or minimally processed foods and culinary ingredients made at home, a cafeteria, or food service operation such as hummus; salsa; salads; mixed vegetables; stir fry; mashed potatoes; soups; casseroles; cooked meats, poultry, or fish; pies, cakes, and cookies; and coffee, tea and lemonade.

⁷⁹ Monteiro C.A., Cannon G., Levy R.B. et al. NOVA. The star shines bright. [Food classification. Public health] *World Nutrition*. January-March 2016, 7, 1-3, 28-38.

⁸⁰ Food and Agriculture Organization of the United Nations (2015) Guidelines on the collection of information on food processing through food consumption surveys. Rome: FAO.

⁸¹ Monteiro CA, Cannon G, Levy RB, Claro RM, Moubarac J-C. (2015). Ultra-processing and a new classification of foods. In: Neff R (ed) *Introduction to the US food system: Public health, environment, and equity*. Johns Hopkins Center for a Livable Future, San Francisco, CA: Jossey-Bass, 2015.

⁸² Ultra-processed products may include an assortment of additives or ingredients not typically found in unprocessed/minimally processed and moderately processed foods or culinary ingredients. Examples of substances only found in ultra-processed products include some directly extracted from foods, such as casein, lactose, whey, and gluten, and some derived from further processing of food constituents, such as hydrogenated or interesterified oils, hydrolyzed proteins, soy protein isolate, maltodextrin, invert sugar and high fructose corn syrup.

⁸³ Monteiro C.A., Cannon G., Levy R.B. et al. NOVA. The star shines bright. [Food classification. Public health] *World Nutrition*. January-March 2016, 7, 1-3, 28-38.

⁸⁴ Food and Agriculture Organization of the United Nations (2015) Guidelines on the collection of information on food processing through food consumption surveys. Rome: FAO.

⁸⁵ Monteiro CA, Cannon G, Levy RB, Claro RM, Moubarac J-C. (2015). Ultra-processing and a new classification of foods. In: Neff R (ed) *Introduction to the US food system: Public health, environment, and equity*. Johns Hopkins Center for a Livable Future, San Francisco, CA: Jossey-Bass, 2015.

⁸⁶ Classes of additives that may infrequently be added to foods and beverages in this category include nutrient supplements, curing and pickling agents, stabilizers (in fluid milk or yogurt only), and anti-oxidants or antimicrobial agents to preserve original properties or prevent microorganism proliferation.

⁸⁷ Nutrient Profile Model. (2016). Pan American Health Organization.

Appendix IX– CCDOC Non-Employee Credentials Policy and Application



Non-Employee Identification Procedure

200.1 PURPOSE AND SCOPE

This procedure provides guidelines for the issuance of identification to non-employees. It is necessary that individuals who enter the facility and the agency represented, understand the rules and security requirements of the Cook County Department of Corrections.

200.1.1 DEFINITIONS

Definitions related to this procedure include:

Non-Employee Identification – An issued photo identification for any person who is not employed by the Cook County Sheriff's Office (e.g., contractors, volunteers, vendors, church groups, diplomats, other non-employees), and color-coded to signify authorization to access non-public areas of the Department, valid for the specified time period only.

Agency- A business, organization or government agency providing a particular service to include, but not limited to, not-for-profit organizations, church groups, volunteers, vendors and other contractors.

Sponsor – An appointed Sheriff's Office member responsible for initiating the non-employee identification application process. The sponsor also acts as a liaison between the agency and the Department (e.g., Facilities Coordinator for Department of Facilities Management, Executive Office for Cermak Health Services).

200.2 POLICY

The Department of Corrections will uphold the safety and security of the facility by conducting a comprehensive criminal background check for each individual entering the Department. The Executive Director and/or the Chief of Staff/Chief of Operations will have the authority to grant immediate and/or special access, and give final determination on appeals. The Department reserves the right to revoke non-employee identification at any time.

200.3 RESPONSIBILITIES

200.3.1 SPONSORS

- (a) The department head shall assign a sponsor who shall be responsible for meeting with applicants and the agency, when practicable.
- (b) The sponsor shall provide the agency with the Agency Agreement Form and once completed, submit the form to the Credentials Unit to retain in the agency's file.
- (c) For new non-employee identification or renewal, the sponsor shall forward the following information to the Executive Office:
 1. Applicants name;
 2. Agency;
 3. Access level (locations);

Cook County Department of Corrections

Cook County DOC Procedures Manual

Non-Employee Identification Procedure

4. Expiration date (e.g., default one year, two years maximum); and
 5. Application
- (d) Once approved the information shall be forwarded to the Credentials Unit via email to CCSO.Credentials@cookcountyil.gov prior to the applicants scheduled arrival.
 - (e) If an applicant is denied, the sponsor may appeal the denial decision, in writing, within five days. The sponsor shall forward all appeals to the Chief of Operations or the authorized designee for an evaluation and determination if access will be granted or the decision to deny is upheld.
 - (f) When notified of a change in status of an applicant/non-employee, the sponsor shall provide immediate notification to the Credentials Unit and the Executive Director's Office, and when practicable, collect the identification from the non-employee.
 - (g) The sponsor shall, when practicable, notify the appropriate agency of any reports of prohibited activity by the non-employee.
 1. If a non-employee's identification has been revoked based on the criteria included in the Application Denial/Revocation Criteria Form, the sponsor shall notify the non-employee and the agency he/she represents and the Credentials Unit.
 - (h) The sponsor shall submit any equipment request received from the applicant to the Executive Director's Office and notify the applicant if approved or denied.

200.3.2 APPLICANT

- (a) The applicant can obtain a non-employee identification by presenting an application to the Credentials Unit, upon approval from the sponsor.
- (b) The applicant must be at least 18 years of age to submit an application to the Credentials Unit.
- (c) The applicant may not submit an application to represent more than one agency unless authorized by the Chief of Operations.
- (d) The applicant shall ensure the application, including all required documents, contains accurate information, and is completed and signed.
- (e) If after receipt of the non-employee identification, the non-employee does not report for three consecutive months with no contact with the sponsor, the identification will be revoked by the sponsor, unless a valid reason is provided.
- (f) An applicant shall submit all equipment requests (e.g. tools, electronic devices) to the sponsor with a copy of the non-employee identification.
- (g) The applicant shall only use a non-employee identification to represent the agency indicated on the application.
- (h) Upon expiration of the applicant's non-employee identification, applicant shall return the non-employee identification to the Credentials Unit within 10 days of expiration.

Cook County Department of Corrections

Cook County DOC Procedures Manual

Non-Employee Identification Procedure

200.3.3 CREDENTIALS UNIT

The Credentials Unit shall process the application, conduct a comprehensive criminal background check, fingerprint and create a photo identification for the applicant.

If an applicant's eligibility is unclear and/or denied as a result of the criminal background inquiry, the Credentials Unit shall notify the applicant that his/her request cannot be processed at this time. The Credential Unit shall also notify the sponsor, the Chief of Operations, and the Correctional Information and Investigations Division (CIID) and give reason for denial.

The Credentials Unit shall also notify the Chief of Operations or the authorized designee and the Correctional Information and Investigations Division (CIID) when a non-employee's identification has been revoked based on the criteria included in the Application Denial/Revocation Criteria Form.

200.4 IMMEDIATE AND/OR DAILY ACCESS

Certain situations may require prompt and/or daily access to the Department, including but not limited to:

- (a) Emergency repairs;
- (b) Replacement, back-up, or substitute individuals (e.g., regular speaker, teacher, repairman);
- (c) Media events;
- (d) Preplanned tours;
- (e) Preplanned meetings; or
- (f) Program events.

In these situations, the Credentials Unit shall follow the process for new/renewal applicants. The Credentials Unit will obtain a copy of current driver's license or state identification, excluding the fingerprint requirement.

Each individual granted such access shall be escorted at all times inside non-public areas of the Department by the sponsor or the authorized designee.

200.5 LOST/STOLEN/DAMAGED CREDENTIALS

In the event of a lost or stolen non-employee identification, regardless of validity, the non-employee shall:

- (a) File a report with a law enforcement agency in the jurisdiction in which the identification was lost and obtain a copy of the report. Reports should contain a report number and a narrative to be accepted; and
- (b) Complete a memorandum and submit a copy of the report to the sponsor.
- (c) Once approved, a payment is required by certified check or money order for the replacement cost of the identification. Current replacement cost is \$20.00.

Cook County Department of Corrections

Cook County DOC Procedures Manual

Non-Employee Identification Procedure

The sponsor shall submit both the memorandum and the report to the Credentials Unit and the Chief of Operations or the authorized designee for approval of a replacement identification.

Any non-employee has the duty to return any found identification to the Credentials Unit without delay. A non-employee who locates a lost/stolen identification within 24 hours of being issued a replacement identification must make prompt notification to the Credentials Unit and return any issued identification to recover the replacement cost. Any non-employee identification that is found at a later date shall be returned to the Credentials Unit; the replacement cost will not be reimbursed to the affected non-employee.

In the event an identification is damaged, the non-employee shall make notification to the sponsor through a memorandum. Upon approval from the sponsor, the non-employee shall surrender the damaged identification to the Credentials Unit for a replacement at a fee.

CONTRABAND

It is a criminal offense to bring contraband into a penal institution. Visitors who bring, attempt to bring or leave an item of contraband in the Cook County Department of Corrections (CCDOC) shall be charged criminally with "Bringing Contraband into a Penal Institution," 720 ILCS 5/31 A.1. The CCDOC has determined contraband to be, but not limited to, the following items:

1. Weapons, explosive devices, ammunition or any item that could cause great bodily harm (*e.g., TASERs, stun guns, firearms, grenades, bombshells*)
2. Knives of any kind
3. Imitation weapons, explosive devices, or any item construed or shaped as a weapon
4. Toxic, hazardous materials or chemicals of any type (*e.g., flammable or combustible liquids, oil*)
5. All tools except those authorized for use by the CCDOC
6. Insecticide, pesticide or herbicide
7. Non-plastic eating utensils
8. Wire, wire rope, rope, string or twine
9. Razors or razor blades
10. Dental floss
11. Aerosol cans
12. Steel, aluminum, aluminum foil, tin, or other metal object
13. Wax, clay or any substance that could be used as a "mold"
14. Glass or glass objects (*other than prescription lenses*)
15. Glue, adhesive or masking tape
16. Intoxicants or alcoholic beverages, ingredients, formulas, or instructions that are used to make intoxicants or alcohol (*e.g., distilled spirits, beer, wine.*)
17. Illegal drugs or drug paraphernalia
18. Hypodermic needles or syringes (*unless accompanied by a prescription*)
19. Plastic or metal instrument modified for use other than its intended purpose
20. Maps or travel tickets (*e.g., airline, train, bus*)
21. Flowers (*dried or fresh*), weeds or foliage
22. Nail files or nail clippers
23. Scissors unless authorized by the CCDOC
24. Paper clips unless authorized by the CCDOC
25. Chewing gum
26. Electronic cigarettes, cigarettes, cigars or any tobacco product (*e.g., rolling paper, loose tobacco*)
27. Incendiary devices (*e.g., lighters, matches*)
28. Radios or video recording devices
29. Recording or pre-recorded audio or video magnetic tapes (*e.g., CDs, DVDs*)
30. Televisions unless authorized by the CCDOC
31. Pagers unless authorized by the CCDOC
32. Paint
33. Gambling devices (*e.g., dice, poker chips*)
34. Mirrors
35. Electronic devices, including cellular phones and technical manuals unless authorized by the Executive Director
36. Computers and equipment unless authorized for use by the Executive Director (*e.g., CDs, DVDs, storage drives, flash drives, memory cards, monitors, keyboards, mice, cables, software, manuals*)
37. Cameras and equipment unless authorized by the Executive Director (*e.g., memory cards, cables, software*)
38. Food preparation equipment unless authorized by the Executive Director (*e.g., coffee makers, hot plates*)
39. Books, magazines, newspapers or pornographic/nude materials, unless authorized by the CCDOC
40. Wearable electronic devices including smart watches



**COOK COUNTY SHERIFF'S OFFICE VNON-
NON-EMPLOYEE/VOLUNTEER APPLICATION**

APPLICANT INFORMATION

TYPE OF REQUEST:

☐ NEW ☐ RENEWAL ☐ CLINICAL ROTATION ☐ TEMPORARY - UNDER 30 DAYS ☐ OTHER:

APPLICANT'S NAME

DATE OF BIRTH:

SSN - LAST 4 DIGITS ONLY

ADDRESS (INCLUDE STREET, CITY, STATE, ZIP CODE):

HOME PHONE:

WORK PHONE:

CELL PHONE:

HEIGHT

WEIGHT

HAIR COLOR

EYE COLOR:

DRIVER'S LICENSE / STATE IDENTIFICATION NUMBER:

EMAIL ADDRESS

EMERGENCY CONTACT (NAME):

RELATIONSHIP:

ADDRESS (INCLUDE STREET, CITY, STATE, ZIP CODE):

EMERGENCY CONTACT NUMBER:

DEPARTMENT APPLICANT IS REQUESTING TO VOLUNTEER WITH:

☐ CCSPD ☐ CSD ☐ CCDOC ☐ EXECUTIVE OFFICE ☐ OTHER:

☒ **N/A**

SPONSOR / VOLUNTEER'S AGENCY (If applicable)

SPONSOR / VOLUNTEER AGENCY NAME:

SPONSOR / VOLUNTEER AGENCY SUPERVISOR (NAME):

CELL PHONE:

CRIMINAL / CIVIL HISTORY (If you answered YES to any questions below, explain on back)

HAVE YOU EVER BEEN ARRESTED?

☐ YES ☐ NO If YES, Date(s):

HAVE YOU EVER BEEN CONVICTED OF A MISDEMEANOR OR FELONY?

☐ YES ☐ NO If YES, Date(s):

DO YOU HAVE A CRIMINAL CASE PENDING AGAINST YOU?

☐ YES ☐ NO If YES, Date(s):

DO YOU HAVE A CIVIL CASE PENDING AGAINST YOU?

☐ YES ☐ NO If YES, Date(s):

DO YOU HAVE A FAMILY MEMBER / FRIEND IN SHERIFF'S OFFICE CUSTODY?

☐ YES ☐ NO If YES, Location(s):

HAVE YOU EVER VISITED AN INMATE?

☐ YES ☐ NO If YES, Date(s):

By signing below, I certify that:

1. The Cook County Sheriff's Office Code of Conduct Agreement has been read and is understood.

Initials

2. I understand that any violation of the Code of Conduct stipulations may result in revocation of privileges, and may include criminal charges.

Initials

3. Non-employee identification issued by the Cook County Sheriff's Office shall remain the property of the Sheriff's Office.

Initials

4. I understand there inherit risks involved with entering a secure facility which may house subjects in custody.

Initials

5. I authorize the Cook County Sheriff's Office to run a complete criminal history background check, including a fingerprint inquiry.

Initials

APPLICANT SIGNATURE:

DATE:

APPROVAL

☐ APPROVED
☐ DENIED

BII SUPERVISOR / DESIGNEE (SIGNATURE):

DATE:

☐ APPROVED
☐ DENIED

BII SUPERVISOR / DESIGNEE (SIGNATURE):

DATE:

VOLUNTEER STATEMENT

Please indicate why you would like to volunteer with/for the Cook County Sheriff's Office and what it is you are seeking from this opportunity:

CRIMINAL / CIVIL HISTORY CONTINUATION

If you answered YES, to any of the criminal/civil history questions, explain below:



COOK COUNTY SHERIFF'S OFFICE CODE OF CONDUCT AGREEMENT

The following generalized rules and regulations are intended as a guide while utilizing on-site facilities of the Cook County Department of Corrections (CCDOC). You are responsible through your affiliation supervisor to the CCDOC Executive Director or the authorized designee. Initial the below listed rules and regulations indicating you have read and understand them:

INITIAL:	No unauthorized contact, conversations including telephone, or interaction with individuals in custody or their family or friends. You are prohibited from trading, bartering, lending or otherwise engaging in any personal transactions with any inmate. You will not share or disclose any information to those in custody.
INITIAL:	You are subject to a search upon entrance and at any time while on the premises. All items, packages, purses, and bags must be placed on the x-ray machine for inspection and may be searched. There are no exceptions to the search procedures. Search and/or questioning by CCDOC sworn members may occur at any time. Failure to cooperate may be grounds for revocation of your access to the facility.
INITIAL:	Attempts to enter a penal institution with contraband will result in prosecution. Contraband includes illegal items such as unlawful drugs, drug paraphernalia, and firearms as well as legally possessed prohibited items such as medication, knives, blades and ammunition. Items secured as contraband are not returnable after seizure. I have received and read the list of prohibited items.
INITIAL:	Mobile communication devices (e.g., cell phones, tablets, smart phones, smart watch) and recording devices (e.g., cameras, digital/tape recorders) are not permitted and are considered contraband unless approved. Written authorization, issued by the CCDOC, shall be carried on your person at all times.
INITIAL:	You are required to immediately notify your sponsor of any involvement with law enforcement as an arrestee, witness, victim, a party in a civil action or any involvement that may jeopardize volunteer status with the CCDOC.
INITIAL:	Termination from your employer is grounds for immediate and automatic revocation of your non-employee identification card. You shall not attempt to use your identification card after being terminated from your employer.
INITIAL:	The CCDOC reserves the right to deny and/or revoke access into any of its facilities. Violation of any agreed stipulations may result in revocation of privileges as well as criminal prosecution.
INITIAL:	No loitering or deviation from direct routes to and from authorized destinations is permitted. Attempts to access unauthorized areas will result in revocation of access.
INITIAL:	Display your non-employee identification card at all times. Access is limited to a division or area for which authorization is received and only for the purpose authorized.
INITIAL:	Discrimination, harassment, and sexual harassment are strictly prohibited and are grounds for revocation of access and may result in criminal prosecution.
INITIAL:	Wear appropriate attire that meets the safety, image and functionality for the particular role/position. Inappropriate attire includes but not limited to, shorts, mini-skirts/dresses, sheer pants/tops, gang affiliated or representation of gang clothing, colors, hats, etc. You may be denied entry on the basis of improper attire.
INITIAL:	You must notify respective sponsor if a friend or family member is in the custody of the CCDOC or of affiliation with known offenders.
INITIAL:	Notify the immediate CCDOC supervisor if a friend/family member in the custody of the CCDOC is present during a program or in your designated work area. Under no circumstances are you to deviate from the program as established through your sponsor at the CCDOC without prior approval and proper notice of your sponsor.
INITIAL:	Under the provisions of the Prison Rape Elimination Act (PREA) of 2003 (42 USC 147), any instance of sexual contact towards individuals in custody will result in criminal charges.
INITIAL:	Follow all rules regarding tool inventory and control, including keeping your tools and an accurate tool inventory sheet with you at all times. Be aware of your surroundings and be vigilant with any and all tools and materials you have with you in a correctional facility.
INITIAL:	I understand that membership in a known criminal organization shall prohibit me from access. By initialing here, I affirm that I am not a member of or associated with a gang or other known criminal organization.
INITIAL:	I understand that visitation of inmates in custody is prohibited, unless approved by the Executive Director or the authorized designee in accordance with current Department policy and procedure.
INITIAL:	In the event of a lost or stolen non-employee identification credentials, I must file a police report in the jurisdiction in which the identification was lost. The report, along with a memorandum, shall be forwarded to the sponsor and the Sheriff's Office along with a certified check or money order payable to the Cook County Sheriff's Office. The current replacement cost is \$20.00.

BY SIGNING BELOW, I CERTIFY I HAVE READ AND UNDERSTAND THE ABOVE LISTED RULES AND REGULATIONS.

NAME (PRINT)	SIGNATURE:	DATE:
WITNESS (PRINT)	SIGNATURE:	DATE:



**COOK COUNTY SHERIFF'S OFFICE
VOLUNTEER DENIAL CRITERIA**

An applicant's eligibility will be denied if any of the following criteria appears in his/her criminal background check:

1. Current felony or misdemeanor case pending in any court.
2. Active warrant(s).
3. Member or associate of a known criminal organization.
4. Falsifying or omitting information on the application, including but not limited to, identity theft, criminal history, and/or failure to report any current or prior relationship with an inmate.
5. Currently on probation or parole (individual exceptions may apply).
6. Has been in the custody of the CCDOC, Illinois Department of Corrections (IDOC) or any other verified correctional facility in the last three years for any reason.
7. Previous denial or revocation of non-employee identification.
8. Violent criminal history, drug charges and/or sex offenses to include registered sex offender (current charge, prior conviction, arrest history), any felonies in the past 10 years and/or any misdemeanors in the past three years, from the date of the conviction or the last day of sentence, whichever is later.
9. Civil or administrative adjudications resulting from sexual misconduct, including any court ordered protective order.
10. Evidence that the individual does not meet the conduct and ethics standards established by the Sheriff's Office.

A non-employee's identification can be revoked based on the following criteria:

1. Violating the Code of Conduct Agreement.
2. No longer employed by or a volunteer of the agency requesting access.
3. Found in an unauthorized area.
4. Use of identification for purposes other than intended.
5. Any arrest since issuance.
6. Found to have violated any of the non-employee identification standards.
7. Failure to report for three consecutive months.

(ATTACHMENT)

Appendix X – Economic Disclosure Forms



**COOK COUNTY
ECONOMIC DISCLOSURE STATEMENT
AND EXECUTION DOCUMENT
INDEX**

Section	Description	Pages
1	Instructions for Completion of EDS	EDS i - ii
2	Certifications	EDS 1– 2
3	Economic and Other Disclosures, Affidavit of Child Support Obligations, Disclosure of Ownership Interest and Familial Relationship Disclosure Form	EDS 3 – 12
4	Cook County Affidavit for Wage Theft Ordinance	EDS 13-14
5	Contract and EDS Execution Page	EDS 15
6	Cook County Signature Page	EDS 16

SECTION 1
INSTRUCTIONS FOR COMPLETION OF
ECONOMIC DISCLOSURE STATEMENT AND EXECUTION DOCUMENT

This Economic Disclosure Statement and Execution Document ("EDS") is to be completed and executed by every Bidder on a County contract, every Proposer responding to a Request for Proposals, and every Respondent responding to a Request for Qualifications, and others as required by the Chief Procurement Officer. The execution of the EDS shall serve as the execution of a contract awarded by the County. The Chief Procurement Officer reserves the right to request that the Bidder or Proposer, or Respondent provide an updated EDS on an annual basis.

Definitions. Terms used in this EDS and not otherwise defined herein shall have the meanings given to such terms in the Instructions to Bidders, General Conditions, Request for Proposals, Request for Qualifications, as applicable.

Affiliate means a person that directly or indirectly through one or more intermediaries, Controls is Controlled by, or is under common Control with the Person specified.

Applicant means a person who executes this EDS.

Bidder means any person who submits a Bid.

Code means the Code of Ordinances, Cook County, Illinois available on municode.com.

Contract shall include any written document to make Procurements by or on behalf of Cook County.

Contractor or *Contracting Party* means a person that enters into a Contract with the County.

Control means the unfettered authority to directly or indirectly manage governance, administration, work, and all other aspects of a business.

EDS means this complete Economic Disclosure Statement and Execution Document, including all sections listed in the Index and any attachments.

Joint Venture means an association of two or more Persons proposing to perform a for-profit business enterprise. Joint Ventures must have an agreement in writing specifying the terms and conditions of the relationship between the partners and their relationship and respective responsibility for the Contract

Lobby or *lobbying* means to, for compensation, attempt to influence a County official or County employee with respect to any County matter.

Lobbyist means any person who lobbies.

Person or *Persons* means any individual, corporation, partnership, Joint Venture, trust, association, Limited Liability Company, sole proprietorship or other legal entity.

Prohibited Acts means any of the actions or occurrences which form the basis for disqualification under the Code, or under the Certifications hereinafter set forth.

Proposal means a response to an RFP.

Proposer means a person submitting a Proposal.

Response means response to an RFQ.

Respondent means a person responding to an RFQ.

RFP means a Request for Proposals issued pursuant to this Procurement Code.

RFQ means a Request for Qualifications issued to obtain the qualifications of interested parties.

**INSTRUCTIONS FOR COMPLETION OF
ECONOMIC DISCLOSURE STATEMENT AND EXECUTION DOCUMENT**

Section 1: Instructions. Section 1 sets forth the instructions for completing and executing this EDS.

Section 2: Certifications. Section 2 sets forth certifications that are required for contracting parties under the Code and other applicable laws. Execution of this EDS constitutes a warranty that all the statements and certifications contained, and all the facts stated, in the Certifications are true, correct and complete as of the date of execution.

Section 3: Economic and Other Disclosures Statement. Section 3 is the County's required Economic and Other Disclosures Statement form. Execution of this EDS constitutes a warranty that all the information provided in the EDS is true, correct and complete as of the date of execution, and binds the Applicant to the warranties, representations, agreements and acknowledgements contained therein.

Required Updates. The Applicant is required to keep all information provided in this EDS current and accurate. In the event of any change in the information provided, including but not limited to any change which would render inaccurate or incomplete any certification or statement made in this EDS, the Applicant shall supplement this EDS up to the time the County takes action, by filing an amended EDS or such other documentation as is required.

Additional Information. The County's Governmental Ethics and Campaign Financing Ordinances impose certain duties and obligations on persons or entities seeking County contracts, work, business, or transactions, and the Applicant is expected to comply fully with these ordinances. For further information please contact the Director of Ethics at (312) 603-4304 (69 W. Washington St. Suite 3040, Chicago, IL 60602) or visit the web-site at cookcountyil.gov/ethics-board-of.

Authorized Signers of Contract and EDS Execution Page. If the Applicant is a corporation, the President and Secretary must execute the EDS. In the event that this EDS is executed by someone other than the President, attach hereto a certified copy of that section of the Corporate By-Laws or other authorization by the Corporation, satisfactory to the County that permits the person to execute EDS for said corporation. If the corporation is not registered in the State of Illinois, a copy of the Certificate of Good Standing from the state of incorporation must be submitted with this Signature Page.

If the Applicant is a partnership or joint venture, all partners or joint venturers must execute the EDS, unless one partner or joint venture has been authorized to sign for the partnership or joint venture, in which case, the partnership agreement, resolution or evidence of such authority satisfactory to the Office of the Chief Procurement Officer must be submitted with this Signature Page.

If the Applicant is a member-managed LLC all members must execute the EDS, unless otherwise provided in the operating agreement, resolution or other corporate documents. If the Applicant is a manager-managed LLC, the manager(s) must execute the EDS. The Applicant must attach either a certified copy of the operating agreement, resolution or other authorization, satisfactory to the County, demonstrating such person has the authority to execute the EDS on behalf of the LLC. If the LLC is not registered in the State of Illinois, a copy of a current Certificate of Good Standing from the state of incorporation must be submitted with this Signature Page.

If the Applicant is a Sole Proprietorship, the sole proprietor must execute the EDS.

A "Partnership" "Joint Venture" or "Sole Proprietorship" operating under an Assumed Name must be registered with the Illinois county in which it is located, as provided in 805 ILCS 405 (2012), and documentation evidencing registration must be submitted with the EDS.

Effective October 1, 2016 all foreign corporations and LLCs must be registered with the Illinois Secretary of State's Office unless a statutory exemption applies to the applicant. Applicants who are exempt from registering must provide a written statement explaining why they are exempt from registering as a foreign entity with the Illinois Secretary of State's Office.

SECTION 2**CERTIFICATIONS**

THE FOLLOWING CERTIFICATIONS ARE MADE PURSUANT TO STATE LAW AND THE CODE. THE APPLICANT IS CAUTIONED TO CAREFULLY READ THESE CERTIFICATIONS PRIOR TO SIGNING THE SIGNATURE PAGE. SIGNING THE SIGNATURE PAGE SHALL CONSTITUTE A WARRANTY BY THE APPLICANT THAT ALL THE STATEMENTS, CERTIFICATIONS AND INFORMATION SET FORTH WITHIN THESE CERTIFICATIONS ARE TRUE, COMPLETE AND CORRECT AS OF THE DATE THE SIGNATURE PAGE IS SIGNED. THE APPLICANT IS NOTIFIED THAT IF THE COUNTY LEARNS THAT ANY OF THE FOLLOWING CERTIFICATIONS WERE FALSELY MADE, THAT ANY CONTRACT ENTERED INTO WITH THE APPLICANT SHALL BE SUBJECT TO TERMINATION.

A. PERSONS AND ENTITIES SUBJECT TO DISQUALIFICATION

No person or business entity shall be awarded a contract or sub-contract, for a period of five (5) years from the date of conviction or entry of a plea or admission of guilt, civil or criminal, if that person or business entity:

- 1) Has been convicted of an act committed, within the State of Illinois, of bribery or attempting to bribe an officer or employee of a unit of state, federal or local government or school district in the State of Illinois in that officer's or employee's official capacity;
- 2) Has been convicted by federal, state or local government of an act of bid-rigging or attempting to rig bids as defined in the Sherman Anti-Trust Act and Clayton Act. Act. 15 U.S.C. Section 1 *et seq.*;
- 3) Has been convicted of bid-rigging or attempting to rig bids under the laws of federal, state or local government;
- 4) Has been convicted of an act committed, within the State, of price-fixing or attempting to fix prices as defined by the Sherman Anti-Trust Act and the Clayton Act. 15 U.S.C. Section 1, *et seq.*;
- 5) Has been convicted of price-fixing or attempting to fix prices under the laws the State;
- 6) Has been convicted of defrauding or attempting to defraud any unit of state or local government or school district within the State of Illinois;
- 7) Has made an admission of guilt of such conduct as set forth in subsections (1) through (6) above which admission is a matter of record, whether or not such person or business entity was subject to prosecution for the offense or offenses admitted to; or
- 8) Has entered a plea of *nolo contendere* to charge of bribery, price-fixing, bid-rigging, or fraud, as set forth in subparagraphs (1) through (6) above.

In the case of bribery or attempting to bribe, a business entity may not be awarded a contract if an official, agent or employee of such business entity committed the Prohibited Act on behalf of the business entity and pursuant to the direction or authorization of an officer, director or other responsible official of the business entity, and such Prohibited Act occurred within three years prior to the award of the contract. In addition, a business entity shall be disqualified if an owner, partner or shareholder controlling, directly or indirectly, 20% or more of the business entity, or an officer of the business entity has performed any Prohibited Act within five years prior to the award of the Contract.

THE APPLICANT HEREBY CERTIFIES THAT: The Applicant has read the provisions of Section A, Persons and Entities Subject to Disqualification, that the Applicant has not committed any Prohibited Act set forth in Section A, and that award of the Contract to the Applicant would not violate the provisions of such Section or of the Code.

B. BID-RIGGING OR BID ROTATING

THE APPLICANT HEREBY CERTIFIES THAT: In accordance with 720 ILCS 5/33 E-11, neither the Applicant nor any Affiliated Entity is barred from award of this Contract as a result of a conviction for the violation of State laws prohibiting bid-rigging or bid rotating.

C. DRUG FREE WORKPLACE ACT

THE APPLICANT HEREBY CERTIFIES THAT: The Applicant will provide a drug free workplace, as required by (30 ILCS 580/3).

D. DELINQUENCY IN PAYMENT OF TAXES

THE APPLICANT HEREBY CERTIFIES THAT: *The Applicant is not an owner or a party responsible for the payment of any tax or fee administered by Cook County, such as bar award of a contract or subcontract pursuant to the Code, Chapter 34, Section 34-171.*

E. HUMAN RIGHTS ORDINANCE

No person who is a party to a contract with Cook County ("County") shall engage in unlawful discrimination or sexual harassment against any individual in the terms or conditions of employment, credit, public accommodations, housing, or provision of County facilities, services or programs (Code Chapter 42, Section 42-30 *et seq.*).

F. ILLINOIS HUMAN RIGHTS ACT

THE APPLICANT HEREBY CERTIFIES THAT: *It is in compliance with the Illinois Human Rights Act (775 ILCS 5/2-105), and agrees to abide by the requirements of the Act as part of its contractual obligations.*

G. INSPECTOR GENERAL (COOK COUNTY CODE, CHAPTER 34, SECTION 34-174 and Section 34-250)

The Applicant has not willfully failed to cooperate in an investigation by the Cook County Independent Inspector General or to report to the Independent Inspector General any and all information concerning conduct which they know to involve corruption, or other criminal activity, by another county employee or official, which concerns his or her office of employment or County related transaction.

The Applicant has reported directly and without any undue delay any suspected or known fraudulent activity in the County's Procurement process to the Office of the Cook County Inspector General.

H. CAMPAIGN CONTRIBUTIONS (COOK COUNTY CODE, CHAPTER 2, SECTION 2-585)

THE APPLICANT CERTIFIES THAT: It has read and shall comply with the Cook County's Ordinance concerning campaign contributions, which is codified at Chapter 2, Division 2, Subdivision II, Section 585, and can be read in its entirety at www.municode.com.

I. GIFT BAN, (COOK COUNTY CODE, CHAPTER 2, SECTION 2-574)

THE APPLICANT CERTIFIES THAT: It has read and shall comply with the Cook County's Ordinance concerning receiving and soliciting gifts and favors, which is codified at Chapter 2, Division 2, Subdivision II, Section 574, and can be read in its entirety at www.municode.com.

J. LIVING WAGE ORDINANCE PREFERENCE (COOK COUNTY CODE, CHAPTER 34, SECTION 34-160;

Unless expressly waived by the Cook County Board of Commissioners, the Code requires that a living wage must be paid to individuals employed by a Contractor which has a County Contract and by all subcontractors of such Contractor under a County Contract, throughout the duration of such County Contract. The amount of such living wage is annually by the Chief Financial Officer of the County, and shall be posted on the Chief Procurement Officer's website.

The term "Contract" as used in Section 4, I, of this EDS, specifically excludes contracts with the following:

- 1) Not-For Profit Organizations (defined as a corporation having tax exempt status under Section 501(C)(3) of the United States Internal Revenue Code and recognized under the Illinois State not-for-profit law);
- 2) Community Development Block Grants;
- 3) Cook County Works Department;
- 4) Sheriff's Work Alternative Program; and
- 5) Department of Correction inmates.

SECTION 3

REQUIRED DISCLOSURES

1. DISCLOSURE OF LOBBYIST CONTACTS

List all persons that have made lobbying contacts on your behalf with respect to this contract:

Name	Address

2. LOCAL BUSINESS PREFERENCE STATEMENT (CODE, CHAPTER 34, SECTION 34-230)

Local business means a Person, including a foreign corporation authorized to transact business in Illinois, having a bona fide establishment located within the County at which it is transacting business on the date when a Bid is submitted to the County, and which employs the majority of its regular, full-time work force within the County. A Joint Venture shall constitute a Local Business if one or more Persons that qualify as a "Local Business" hold interests totaling over 50 percent in the Joint Venture, even if the Joint Venture does not, at the time of the Bid submittal, have such a bona fide establishment within the County.

- a) Is Applicant a "Local Business" as defined above?
- Yes: _____ No: _____

- b) If yes, list business addresses within Cook County:
- _____
- _____
- _____

- c) Does Applicant employ the majority of its regular full-time workforce within Cook County?
- Yes: _____ No: _____

3. THE CHILD SUPPORT ENFORCEMENT ORDINANCE (CODE, CHAPTER 34, SECTION 34-172)

Every Applicant for a County Privilege shall be in full compliance with any child support order before such Applicant is entitled to receive or renew a County Privilege. When delinquent child support exists, the County shall not issue or renew any County Privilege, and may revoke any County Privilege.

All Applicants are required to review the Cook County Affidavit of Child Support Obligations attached to this EDS (EDS-5) and complete the Affidavit, based on the instructions in the Affidavit.

4. REAL ESTATE OWNERSHIP DISCLOSURES.

The Applicant must indicate by checking the appropriate provision below and providing all required information that either:

- a) The following is a complete list of all real estate owned by the Applicant in Cook County:

PERMANENT INDEX NUMBER(S): _____

**(ATTACH SHEET IF NECESSARY TO LIST ADDITIONAL INDEX
NUMBERS)**

OR:

- b) _____The Applicant owns no real estate in Cook County.

5. EXCEPTIONS TO CERTIFICATIONS OR DISCLOSURES.

If the Applicant is unable to certify to any of the Certifications or any other statements contained in this EDS and not explained elsewhere in this EDS, the Applicant must explain below:

If the letters, "NA", the word "None" or "No Response" appears above, or if the space is left blank, it will be conclusively presumed that the Applicant certified to all Certifications and other statements contained in this EDS.

COOK COUNTY AFFIDAVIT OF CHILD SUPPORT OBLIGATIONS

Effective July 1, 1998, every applicant for a County Privilege shall be in full compliance with any Child Support Order before such applicant is entitled to receive a County Privilege. When Delinquent Child Support Exists, the County shall not issue or renew any County Privilege, and may revoke any County Privilege.

"Applicant" means any person or business entity, **including all Substantial Owners**, seeking issuance of a County Privilege or renewal of an existing County Privilege from the County. This term shall not include any political subdivision of the federal or state government, including units of local government, and not-for-profit organizations.

"County Privilege" means any business license, including but not limited to liquor dealers' licenses, packaged goods licenses, tavern licenses, restaurant licenses, and gun licenses; real property license or lease; permit, including but not limited to building permits, zoning permits or approvals; environmental certificate; County HOME Loan, and contracts exceeding the value of \$10,000.00.

"Substantial Owner" means any person or persons who own or hold a twenty-five percent (25%) or more percentage of interest in any business entity seeking a County Privilege, including those shareholders, general or limited partners, beneficiaries and principals; except where a business entity is an individual or sole proprietorship, Substantial Owner means that individual or sole proprietor.

All Applicants/Substantial Owners are required to complete this affidavit and comply with the Child Support Enforcement Ordinance before any privilege is granted. Signature of this form constitutes a certification the information provided below is correct and complete, and that the individual(s) signing this form has/have personal knowledge of such information.

Privilege Information:

Contract #:

County Department:

Business Entity Information (INCLUDES CORPORATE APPLICANT AND CORPORATE SUBSTANTIAL OWNERS):

Business Entity Name: _____

Street Address: _____

City: _____

State: _____

Zip: _____

Phone #: _____

Individual Applicant and Individual Substantial Owner Information (If Applicable):

Last name: _____ First Name: _____ MI: _____

SS# (Last Four Digits): _____ Date of Birth: _____

Street Address: _____

City: _____ State: _____ Zip: _____

Home Phone: (____) ____ - ____ Driver's License No: _____

Child Support Obligation Information:

The Applicant, being duly sworn on oath or affirmation hereby states that to the best of my knowledge (place an "X" next to "A", "B", or "C").

- _____ A. The Applicant has no judicially or administratively ordered child support obligations.
- _____ B. The Applicant has an outstanding judicially or administratively ordered obligation, but is paying in accordance with the terms of the order.
- _____ C. The Applicant is delinquent in paying judicially or administratively ordered child support obligations

The Applicant understands that failure to disclose any judicially or administratively ordered child support debt owed will be grounds for revoking the privilege.

Name: _____

Signature: _____

Date: _____

Subscribed and sworn to before me this _____ day of _____, 20____

X _____

Notary Public Signature**Notary Seal**

Note: The above information is subject to verification prior to the award of the contract.

COOK COUNTY DISCLOSURE OF OWNERSHIP INTEREST STATEMENT

The Cook County Code of Ordinances (§2-610 *et seq.*) requires that any Applicant for any County Action must disclose information concerning ownership interests in the Applicant. This Disclosure of Ownership Interest Statement must be completed with all information current as of the date this Statement is signed. Furthermore, this Statement must be kept current, by filing an amended Statement, until such time as the County Board or County Agency shall take action on the application. The information contained in this Statement will be maintained in a database and made available for public viewing. **County reserves the right to request additional information to verify veracity of information contained in this statement.**

If you are asked to list names, but there are no applicable names to list, you must state NONE. An incomplete Statement will be returned and any action regarding this contract will be delayed. A failure to fully comply with the ordinance may result in the action taken by the County Board or County Agency being voided.

"Applicant" means any Entity or person making an application to the County for any County Action.

"County Action" means any action by a County Agency, a County Department, or the County Board regarding an ordinance or ordinance amendment, a County Board approval, or other County agency approval, with respect to contracts, leases, or sale or purchase of real estate.

"Person" "Entity" or "Legal Entity" means a sole proprietorship, corporation, partnership, association, business trust, estate, two or more persons having a joint or common interest, trustee of a land trust, other commercial or legal entity or any beneficiary or beneficiaries thereof.

This Disclosure of Ownership Interest Statement must be submitted by :

1. An Applicant for County Action and
2. A Person that holds stock or a beneficial interest in the Applicant and is listed on the Applicant's Statement (a "Holder") must file a Statement and complete #1 only under **Ownership Interest Declaration**.

Please print or type responses clearly and legibly. Add additional pages if needed, being careful to identify each portion of the form to which each additional page refers.

This Statement is being made by the ☐ Applicant or ☐ Stock/Beneficial Interest Holder

This Statement is an: ☐ Original Statement or ☐ Amended Statement

Identifying Information:

Name _____

D/B/A: _____ FEIN # Only: _____

Street Address: _____

City: _____ State: _____ Zip Code: _____

Phone No.: _____ Fax Number: _____ Email: _____

Cook County Business Registration Number: _____
(Sole Proprietor, Joint Venture Partnership)

Corporate File Number (if applicable): _____

Form of Legal Entity:

☐ Sole Proprietor ☐ Partnership ☐ Corporation ☐ Trustee of Land Trust

☐ Business Trust ☐ Estate ☐ Association ☐ Joint Venture

☐ Other (describe) _____

Ownership Interest Declaration:

1. List the name(s), address, and percent ownership of each Person having a legal or beneficial interest (including ownership) of more than five percent (5%) in the Applicant/Holder.

Name	Address	Percentage Interest in Applicant/Holder
------	---------	---

2. If the interest of any Person listed in (1) above is held as an agent or agents, or a nominee or nominees, list the name and address of the principal on whose behalf the interest is held.

Name of Agent/Nominee	Name of Principal	Principal's Address
-----------------------	-------------------	---------------------

3. Is the Applicant constructively controlled by another person or Legal Entity? ☐ Yes ☐ No
- If yes, state the name, address and percentage of beneficial interest of such person, and the relationship under which such control is being or may be exercised.

Name	Address	Percentage of Beneficial Interest	Relationship
------	---------	-----------------------------------	--------------

Corporate Officers, Members and Partners Information:

For all corporations, list the names, addresses, and terms for all corporate officers. For all limited liability companies, list the names, addresses for all members. For all partnerships and joint ventures, list the names, addresses, for each partner or joint venture.

Name	Address	Title (specify title of Office, or whether manager or partner/joint venture)	Term of Office
------	---------	--	----------------

Declaration (check the applicable box):

- ☐ I state under oath that the Applicant has withheld no disclosure as to ownership interest in the Applicant nor reserved any information, data or plan as to the intended use or purpose for which the Applicant seeks County Board or other County Agency action.
- ☐ I state under oath that the Holder has withheld no disclosure as to ownership interest nor reserved any information required to be disclosed.

COOK COUNTY DISCLOSURE OF OWNERSHIP INTEREST STATEMENT SIGNATURE PAGE

Name of Authorized Applicant/Holder Representative (please print or type)

Signature

E-mail address

Subscribed to and sworn before me
this _____ day of _____, 20__.

X _____
Notary Public Signature

Title

Date

Phone Number

My commission expires:

Notary Seal



COOK COUNTY BOARD OF ETHICS
 69 W. WASHINGTON STREET, SUITE 3040
 CHICAGO, ILLINOIS 60602
 312/603-4304 Office 312/603-9988 Fax

FAMILIAL RELATIONSHIP DISCLOSURE PROVISION

Nepotism Disclosure Requirement:

Doing a significant amount of business with the County requires that you disclose to the Board of Ethics the existence of any familial relationships with any County employee or any person holding elective office in the State of Illinois, the County, or in any municipality within the County. The Ethics Ordinance defines a significant amount of business for the purpose of this disclosure requirement as more than \$25,000 in aggregate County leases, contracts, purchases or sales in any calendar year.

If you are unsure of whether the business you do with the County or a County agency will cross this threshold, err on the side of caution by completing the attached familial disclosure form because, among other potential penalties, any person found guilty of failing to make a required disclosure or knowingly filing a false, misleading, or incomplete disclosure will be prohibited from doing any business with the County for a period of three years. The required disclosure should be filed with the Board of Ethics by January 1 of each calendar year in which you are doing business with the County and again with each bid/proposal/quotation to do business with Cook County. The Board of Ethics may assess a late filing fee of \$100 per day after an initial 30-day grace period.

The person that is doing business with the County must disclose his or her familial relationships. If the person on the County lease or contract or purchasing from or selling to the County is a business entity, then the business entity must disclose the familial relationships of the individuals who are and, during the year prior to doing business with the County, were:

- its board of directors,
- its officers,
- its employees or independent contractors responsible for the general administration of the entity,
- its agents authorized to execute documents on behalf of the entity, and
- its employees who directly engage or engaged in doing work with the County on behalf of the entity.

Do not hesitate to contact the Board of Ethics at (312) 603-4304 for assistance in determining the scope of any required familial relationship disclosure.

Additional Definitions:

“Familial relationship” means a person who is a spouse, domestic partner or civil union partner of a County employee or State, County or municipal official, or any person who is related to such an employee or official, whether by blood, marriage or adoption, as a:

Parent	Grandparent	Stepfather
Child	Grandchild	Stepmother
Brother	Father-in-law	Stepson
Sister	Mother-in-law	Stepdaughter
Aunt	Son-in-law	Stepbrother
Uncle	Daughter-in-law	Stepsister
Niece	Brother-in-law	Halfbrother
Nephew	Sister-in-law	Halfsister

**COOK COUNTY BOARD OF ETHICS
FAMILIAL RELATIONSHIP DISCLOSURE FORM**

A. PERSON DOING OR SEEKING TO DO BUSINESS WITH THE COUNTY

Name of Person Doing Business with the County: _____

Address of Person Doing Business with the County: _____

Phone number of Person Doing Business with the County: _____

Email address of Person Doing Business with the County: _____

If Person Doing Business with the County is a Business Entity, provide the name, title and contact information for the individual completing this disclosure on behalf of the Person Doing Business with the County:

B. DESCRIPTION OF BUSINESS WITH THE COUNTY

Append additional pages as needed and for each County lease, contract, purchase or sale sought and/or obtained during the calendar year of this disclosure (or the preceding calendar year if disclosure is made on January 1), identify:

The lease number, contract number, purchase order number, request for proposal number and/or request for qualification number associated with the business you are doing or seeking to do with the County: _____

The aggregate dollar value of the business you are doing or seeking to do with the County: \$_____

The name, title and contact information for the County official(s) or employee(s) involved in negotiating the business you are doing or seeking to do with the County: _____

The name, title and contact information for the County official(s) or employee(s) involved in managing the business you are doing or seeking to do with the County: _____

C. DISCLOSURE OF FAMILIAL RELATIONSHIPS WITH COUNTY EMPLOYEES OR STATE, COUNTY OR MUNICIPAL ELECTED OFFICIALS

Check the box that applies and provide related information where needed

- ☐ The Person Doing Business with the County **is an individual** and there is **no familial relationship** between this individual and any Cook County employee or any person holding elective office in the State of Illinois, Cook County, or any municipality within Cook County.
- ☐ The Person Doing Business with the County **is a business entity** and there is **no familial relationship** between any member of this business entity's board of directors, officers, persons responsible for general administration of the business entity, agents authorized to execute documents on behalf of the business entity or employees directly engaged in contractual work with the County on behalf of the business entity, and any Cook County employee or any person holding elective office in the State of Illinois, Cook County, or any municipality within Cook County.

**COOK COUNTY BOARD OF ETHICS
FAMILIAL RELATIONSHIP DISCLOSURE FORM**

- ☐ The Person Doing Business with the County **is an individual** and **there is a familial relationship** between this individual and at least one Cook County employee and/or a person or persons holding elective office in the State of Illinois, Cook County, and/or any municipality within Cook County. **The familial relationships are as follows:**

Name of Individual Doing Business with the County	Name of Related County Employee or State, County or Municipal Elected Official	Title and Position of Related County Employee or State, County or Municipal Elected Official	Nature of Familial Relationship*
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

If more space is needed, attach an additional sheet following the above format.

- ☐ The Person Doing Business with the County **is a business entity** and **there is a familial relationship** between at least one member of this business entity’s board of directors, officers, persons responsible for general administration of the business entity, agents authorized to execute documents on behalf of the business entity and/or employees directly engaged in contractual work with the County on behalf of the business entity, on the one hand, and at least one Cook County employee and/or a person holding elective office in the State of Illinois, Cook County, and/or any municipality within Cook County, on the other. **The familial relationships are as follows:**

Name of Member of Board of Director for Business Entity Doing Business with the County	Name of Related County Employee or State, County or Municipal Elected Official	Title and Position of Related County Employee or State, County or Municipal Elected Official	Nature of Familial Relationship*
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

Name of Officer for Business Entity Doing Business with the County	Name of Related County Employee or State, County or Municipal Elected Official	Title and Position of Related County Employee or State, County or Municipal Elected Official	Nature of Familial Relationship*
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

Name of Person Responsible for the General Administration of the Business Entity Doing Business with the County	Name of Related County Employee or State, County or Municipal Elected Official	Title and Position of Related County Employee or State, County or Municipal Elected Official	Nature of Familial Relationship*
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
Name of Agent Authorized to Execute Documents for Business Entity Doing Business with the County	Name of Related County Employee or State, County or Municipal Elected Official	Title and Position of Related County Employee or State, County or Municipal Elected Official	Nature of Familial Relationship*
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
Name of Employee of Business Entity Directly Engaged in Doing Business with the County	Name of Related County Employee or State, County or Municipal Elected Official	Title and Position of Related County Employee or State, County or Municipal Elected Official	Nature of Familial Relationship*
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

If more space is needed, attach an additional sheet following the above format.

VERIFICATION: To the best of my knowledge, the information I have provided on this disclosure form is accurate and complete. I acknowledge that an inaccurate or incomplete disclosure is punishable by law, including but not limited to fines and debarment.

Signature of Recipient

Date

SUBMIT COMPLETED FORM TO: Cook County Board of Ethics
69 West Washington Street, Suite 3040, Chicago, Illinois 60602
Office (312) 603-4304 – Fax (312) 603-9988
CookCounty.Ethics@cookcountyil.gov

* Spouse, domestic partner, civil union partner or parent, child, sibling, aunt, uncle, niece, nephew, grandparent or grandchild by blood, marriage (*i.e.* in laws and step relations) or adoption.

SECTION 4

COOK COUNTY AFFIDAVIT FOR WAGE THEFT ORDINANCE

Effective May 1, 2015, every Person, ***including Substantial Owners***, seeking a Contract with Cook County must comply with the Cook County Wage Theft Ordinance set forth in Chapter 34, Article IV, Section 179. Any Person/Substantial Owner, who fails to comply with Cook County Wage Theft Ordinance, may request that the Chief Procurement Officer grant a reduction or waiver in accordance with Section 34-179(d).

"Contract" means any written document to make Procurements by or on behalf of Cook County.

"Person" means any individual, corporation, partnership, Joint Venture, trust, association, limited liability company, sole proprietorship or other legal entity.

"Procurement" means obtaining supplies, equipment, goods, or services of any kind.

"Substantial Owner" means any person or persons who own or hold a twenty-five percent (25%) or more percentage of interest in any business entity seeking a County Privilege, including those shareholders, general or limited partners, beneficiaries and principals; except where a business entity is an individual or sole proprietorship, Substantial Owner means that individual or sole proprietor.

All Persons/Substantial Owners are required to complete this affidavit and comply with the Cook County Wage Theft Ordinance before any Contract is awarded. Signature of this form constitutes a certification the information provided below is correct and complete, and that the individual(s) signing this form has/have personal knowledge of such information. **County reserves the right to request additional information to verify veracity of information contained in this Affidavit.**

I. Contract Information:

Contract Number: _____

County Using Agency (requesting Procurement): _____

II. Person/Substantial Owner Information:

Person (Corporate Entity Name): _____

Substantial Owner Complete Name: _____

FEIN# _____

Date of Birth: _____

E-mail address: _____

Street Address: _____

City: _____

State: _____ Zip: _____

Home Phone: () _____ - _____

III. Compliance with Wage Laws:

Within the past five years has the Person/Substantial Owner, in any judicial or administrative proceeding, been convicted of, entered a plea, made an admission of guilt or liability, or had an administrative finding made for committing a repeated or willful violation of any of the following laws:

Illinois Wage Payment and Collection Act, 820 ILCS 115/1 et seq., YES or NO

Illinois Minimum Wage Act, 820 ILCS 105/1 et seq., YES or NO

Illinois Worker Adjustment and Retraining Notification Act, 820 ILCS 65/1 et seq., YES or NO

Employee Classification Act, 820 ILCS 185/1 et seq., YES or NO

Fair Labor Standards Act of 1938, 29 U.S.C. 201, et seq., YES or NO

Any comparable state statute or regulation of any state, which governs the payment of wages YES or NO

If the Person/Substantial Owner answered "Yes" to any of the questions above, it is ineligible to enter into a Contract with Cook County, but can request a reduction or waiver under **Section IV**.

IV. Request for Waiver or Reduction

If Person/Substantial Owner answered “Yes” to any of the questions above, it may request a reduction or waiver in accordance with Section 34-179(d), provided that the request for reduction of waiver is made on the basis of one or more of the following actions that have taken place:

There has been a bona fide change in ownership or Control of the ineligible Person or Substantial Owner
YES or NO

Disciplinary action has been taken against the individual(s) responsible for the acts giving rise to the violation
YES or NO

Remedial action has been taken to prevent a recurrence of the acts giving rise to the disqualification or default
YES or NO

Other factors that the Person or Substantial Owner believe are relevant.
YES or NO

The Person/Substantial Owner must submit documentation to support the basis of its request for a reduction or waiver. The Chief Procurement Officer reserves the right to make additional inquiries and request additional documentation.

V. Affirmation

The Person/Substantial Owner affirms that all statements contained in the Affidavit are true, accurate and complete.

Signature: _____ Date:_____

Name of Person signing (Print): _____ Title:_____

Subscribed and sworn to before me this _____ day of _____, 20_____

X _____
Notary Public Signature Notary Seal

Note: The above information is subject to verification prior to the award of the Contract.

SECTION 5

CONTRACT AND EDS EXECUTION PAGE
PLEASE EXECUTE THREE ORIGINAL PAGES OF EDS

The Applicant hereby certifies and warrants that all of the statements, certifications and representations set forth in this EDS are true, complete and correct; that the Applicant is in full compliance and will continue to be in compliance throughout the term of the Contract or County Privilege issued to the Applicant with all the policies and requirements set forth in this EDS; and that all facts and information provided by the Applicant in this EDS are true, complete and correct. The Applicant agrees to inform the Chief Procurement Officer in writing if any of such statements, certifications, representations, facts or information becomes or is found to be untrue, incomplete or incorrect during the term of the Contract or County Privilege.

Execution by Corporation

_____ Corporation's Name	_____ President's Printed Name and Signature
_____ Telephone	_____ Email
_____ Secretary Signature	_____ Date

Execution by LLC

_____ LLC Name	_____ *Member/Manager Printed Name and Signature
_____ Date	_____ Telephone and Email

Execution by Partnership/Joint Venture

_____ Partnership/Joint Venture Name	_____ *Partner/Joint Venturer Printed Name and Signature
_____ Date	_____ Telephone and Email

Execution by Sole Proprietorship

_____ Printed Name Signature	_____ Assumed Name (if applicable)
_____ Date	_____ Telephone and Email

Subscribed and sworn to before me this

_____ day of _____, 20____.

My commission expires:

_____ Notary Public Signature	_____ Notary Seal
----------------------------------	----------------------

*If the operating agreement, partnership agreement or governing documents requiring execution by multiple members, managers, partners, or joint venturers, please complete and execute additional Contract and EDS Execution Pages.

SECTION 6
COOK COUNTY SIGNATURE PAGE

ON BEHALF OF THE COUNTY OF COOK, A BODY POLITIC AND CORPORATE OF THE STATE OF ILLINOIS, THIS CONTRACT IS
HEREBY EXECUTED BY:

Cook County Chief Procurement Officer

Date

APPROVED AS TO FORM:

Assistant State's Attorney
(Required on contracts over \$1,000,000)

Date

CONTRACT TERM & AMOUNT

Contract #

Original Contract Term

Renewal Options (If Applicable)

Contract Amount

Cook County Board Approval Date (If Applicable)

Appendix XI – Cook County Contract Agreement



Appendix XII – Addendum Acknowledgement Form



Appendix XIII – MBE/WBE Utilization Plan Forms



MBE/WBE UTILIZATION PLAN - FORM 1

BIDDER/PROPOSER HEREBY STATES that all MBE/WBE firms included in this Plan are certified MBEs/WBEs by at least one of the entities listed in the General Conditions – Section 19.

I. BIDDER/PROPOSER MBE/WBE STATUS: (check the appropriate line)

- ____ Bidder/Proposer is a certified MBE or WBE firm. (If so, attach copy of current Letter of Certification)
- ____ Bidder/Proposer is a Joint Venture and one or more Joint Venture partners are certified MBEs or WBEs. (If so, attach copies of Letter(s) of Certification, a copy of Joint Venture Agreement clearly describing the role of the MBE/WBE firm(s) and its ownership interest in the Joint Venture and a completed Joint Venture Affidavit – available online at www.cookcountyil.gov/contractcompliance)
- ____ Bidder/Proposer is not a certified MBE or WBE firm, nor a Joint Venture with MBE/WBE partners, but will utilize MBE and WBE firms either directly or indirectly in the performance of the Contract. (If so, complete Sections II below and the Letter(s) of Intent – Form 2).

II. ☐ **Direct Participation of MBE/WBE Firms** ☐ **Indirect Participation of MBE/WBE Firms**

NOTE: Where goals have not been achieved through direct participation, Bidder/Proposer shall include documentation outlining efforts to achieve Direct Participation at the time of Bid/Proposal submission. Indirect Participation will only be considered after all efforts to achieve Direct Participation have been exhausted. Only after written documentation of Good Faith Efforts is received will Indirect Participation be considered.

MBEs/WBEs that will perform as subcontractors/suppliers/consultants include the following:

MBE/WBE Firm: _____

Address: _____

E-mail: _____

Contact Person: _____ Phone: _____

Dollar Amount Participation: \$ _____

Percent Amount of Participation: _____ %

*Letter of Intent attached? Yes _____ No _____

*Current Letter of Certification attached? Yes _____ No _____

MBE/WBE Firm: _____

Address: _____

E-mail: _____

Contact Person: _____ Phone: _____

Dollar Amount Participation: \$ _____

Percent Amount of Participation: _____ %

*Letter of Intent attached? Yes _____ No _____

*Current Letter of Certification attached? Yes _____ No _____

Attach additional sheets as needed.

*** Letter(s) of Intent and current Letters of Certification must be submitted at the time of bid.**

MBE/WBE LETTER OF INTENT - FORM 2

M/WBE Firm: _____

Certifying Agency: _____

Contact Person: _____

Certification Expiration Date: _____

Address: _____

Ethnicity: _____

City/State: _____ Zip: _____

Bid/Proposal/Contract #: _____

Phone: _____ Fax: _____

FEIN #: _____

Email: _____

Participation: ☐ Direct ☐ Indirect

Will the M/WBE firm be subcontracting any of the goods or services of this contract to another firm?

☐ No ☐ Yes – Please attach explanation. Proposed Subcontractor(s): _____

The undersigned M/WBE is prepared to provide the following Commodities/Services for the above named Project/ Contract: *(If more space is needed to fully describe M/WBE Firm's proposed scope of work and/or payment schedule, attach additional sheets)*

Indicate the **Dollar Amount**, **Percentage**, and the **Terms of Payment** for the above-described Commodities/ Services:

THE UNDERSIGNED PARTIES AGREE that this Letter of Intent will become a binding Subcontract Agreement for the above work, conditioned upon (1) the Bidder/Proposer's receipt of a signed contract from the County of Cook; (2) Undersigned Subcontractor remaining compliant with all relevant credentials, codes, ordinances and statutes required by Contractor, Cook County, and the State to participate as a MBE/WBE firm for the above work. The Undersigned Parties do also certify that they did not affix their signatures to this document until all areas under Description of Service/ Supply and Fee/Cost were completed.

Signature (M/WBE)

Signature (Prime Bidder/Proposer)

Print Name

Print Name

Firm Name

Firm Name

Date

Date

Subscribed and sworn before me

Subscribed and sworn before me

this ____ day of _____, 20____.

this ____ day of _____, 20____.

Notary Public _____

Notary Public _____

SEAL

SEAL

PETITION FOR REDUCTION/WAIVER OF MBE/WBE PARTICIPATION – FORM 3

A. BIDDER/PROPOSER HEREBY REQUESTS:

☐

FULL MBE WAIVER

☐

FULL WBE WAIVER

☐

REDUCTION (PARTIAL MBE and/or WBE PARTICIPATION)

_____ % of Reduction for MBE Participation

_____ % of Reduction for WBE Participation

B. REASON FOR FULL/REDUCTION WAIVER REQUEST

Bidder/Proposer shall check each item applicable to its reason for a waiver request. Additionally, supporting documentation shall be submitted with this request.

☐

(1) Lack of sufficient qualified MBEs and/or WBEs capable of providing the goods or services required by the contract. **(Please explain)**

☐

(2) The specifications and necessary requirements for performing the contract make it impossible or economically infeasible to divide the contract to enable the contractor to utilize MBEs and/or WBEs in accordance with the applicable participation. **(Please explain)**

☐

(3) Price(s) quoted by potential MBEs and/or WBEs are above competitive levels and increase cost of doing business and would make acceptance of such MBE and/or WBE bid economically impracticable, taking into consideration the percentage of total contract price represented by such MBE and/or WBE bid. **(Please explain)**

☐

(4) There are other relevant factors making it impossible or economically infeasible to utilize MBE and/or WBE firms. **(Please explain)**

C. GOOD FAITH EFFORTS TO OBTAIN MBE/WBE PARTICIPATION

☐

(1) Made timely written solicitation to identified MBEs and WBEs for utilization of goods and/or services; and provided MBEs and WBEs with a timely opportunity to review and obtain relevant specifications, terms and conditions of the proposal to enable MBEs and WBEs to prepare an informed response to solicitation. **(Attach of copy written solicitations made)**

☐

(2) Used the services and assistance of the Office of Contract Compliance staff. **(Please explain)**

☐

(3) Timely notified and used the services and assistance of community, minority and women business organizations. **(Attach of copy written solicitations made)**

☐

(4) Followed up on initial solicitation of MBEs and WBEs to determine if firms are interested in doing business. **(Attach supporting documentation)**

☐

(5) Engaged MBEs & WBEs for direct/indirect participation. **(Please explain)**

D. OTHER RELEVANT INFORMATION

Attach any other documentation relative to Good Faith Efforts in complying with MBE/WBE participation.

Appendix XIV – Identification of Subcontractor/Supplier/Subconsultant Form



Cook County
Office of the Chief Procurement Officer
Identification of Subcontractor/Supplier/Subconsultant Form

OCPO ONLY:

- ☐ Disqualification
☐ Check Complete

The Bidder/Proposer/Respondent ("the Contractor") will fully complete and execute and submit an Identification of Subcontractor/Supplier/Subconsultant Form ("ISF") with each Bid, Request for Proposal, and Request for Qualification. **The Contractor must complete the ISF for each Subcontractor, Supplier or Subconsultant which shall be used on the Contract.** In the event that there are any changes in the utilization of Subcontractors, Suppliers or Subconsultants, the Contractor must file an updated ISF.

Bid/RFP/RFQ No.:	Date:
Total Bid or Proposal Amount:	Contract Title:
Contractor:	Subcontractor/Supplier/ Subconsultant to be added or substitute:
Authorized Contact for Contractor:	Authorized Contact for Subcontractor/Supplier/ Subconsultant:
Email Address (Contractor):	Email Address (Subcontractor):
Company Address (Contractor):	Company Address (Subcontractor):
City, State and Zip (Contractor):	City, State and Zip (Subcontractor):
Telephone and Fax (Contractor):	Telephone and Fax (Subcontractor):
Estimated Start and Completion Dates (Contractor):	Estimated Start and Completion Dates (Subcontractor):

Note: Upon request, a copy of all written subcontractor agreements must be provided to the OCPO.

<u>Description of Services or Supplies</u>	<u>Total Price of Subcontract for Services or Supplies</u>

The subcontract documents will incorporate all requirements of the Contract awarded to the Contractor as applicable. The subcontract will in no way hinder the Subcontractor/Supplier/Subconsultant from maintaining its progress on any other contract on which it is either a Subcontractor/Supplier/Subconsultant or principal contractor. This disclosure is made with the understanding that the Contractor is not under any circumstances relieved of its abilities and obligations, and is responsible for the organization, performance, and quality of work. **This form does not approve any proposed changes, revisions or modifications to the contract approved MBE/WBE Utilization Plan. Any changes to the contract's approved MBE/WBE/Utilization Plan must be submitted to the Office of the Contract Compliance.**

Contractor

Name

Title

Prime Contractor Signature

Date

Appendix XV – IT Special Terms and Conditions

1. Definitions for Special Conditions

1.1. **“Assets”** means Equipment, Software, Intellectual Property, IP Materials and other assets used in providing the Services. Assets are considered in use as of the date of deployment.

1.2. **“Business Associate Agreement”** or **“BAA”** means an agreement that meets the requirements of 45 C.F.R. 164.504(e).

1.3. **“Business Continuity Plan”** means the planned process, and related activities, required to maintain continuity of business operations between the period of time following declaration of a Disaster until such time an IT environment is returned to an acceptable condition of normal business operation.

1.4. **“Cardholder Data”** means data that meets the definition of “Cardholder Data” in the most recent versions of the Payment Card Industry’s Data Security Standard.

1.5. **“Change”** means, in an operational context, an addition, modification or deletion to any Equipment, Software, IT environment, IT systems, network, device, infrastructure, circuit, documentation or other items related to Services. Changes may arise reactively in response to Incidents/Problems or externally imposed requirements (e.g., legislative changes), or proactively from attempts to (a) seek greater efficiency or effectiveness in the provision or delivery of Services; (b) reflect business initiatives; or (c) implement programs, projects or Service improvement initiatives.

1.6. **“Change Management”** means, in an operational context, the Using Agency approved processes and procedures necessary to manage Changes with the goal of enabling Using Agency-approved Changes with minimum disruption.

1.7. **“Change Order”** means a document that authorizes a Change to the Services or Deliverables under the Agreement, whether in time frames, costs, or scope.

1.8. **“Change Request”** means one Party’s request to the other Party for a Change Order.

1.9. **“Contractor”** has the same meaning as either: (a) both “Contractor” and “Consultant” as such terms are defined, and may be interchangeably used in the County’s Professional Services Agreement, if such document forms the basis of this Agreement or (b) “Contractor” as defined in the County’s Instruction to Bidders and General Conditions, if such document forms the basis of this Agreement.

1.10. **“Contractor Confidential Information”** means all non-public proprietary information of Contractor that is marked confidential, restricted, proprietary, or with a similar designation; provided that Contractor Confidential Information excludes: (a) Using Agency Confidential Information, (b) Using Agency Data; (c) information that may be subject to disclosure under Illinois Freedom of Information Act, 5 ILCS 140/1 et seq. or under the Cook County Code of Ordinances; and (d) the terms of this Agreement, regardless of whether marked with a confidential designation or not.

1.11. **“Contractor Facilities”** means locations owned, leased or otherwise utilized by Contractor and its Subcontractors from which it or they may provide Services.

1.12. **“Contractor Intellectual Property”** means all Intellectual Property owned or licensed by

Contractor.

- 1.13. ***“Contractor IP Materials”*** means all IP Materials owned or licensed by Contractor.
- 1.14. ***“Contractor Personnel”*** means any individuals that are employees, representatives, Subcontractors or agents of Contractor, or of a direct or indirect Subcontractor of Contractor.
- 1.15. ***“Contractor-Provided Equipment”*** means Equipment provided by or on behalf of Contractor.”
- 1.16. ***“Contractor-Provided Software”*** means Software provided by or on behalf of Contractor.
- 1.17. ***“Criminal Justice Information”*** means data that meets the definition of “Criminal Justice Information” in the most recent version of FBI’s CJIS Security Policy and also data that meets the definition of “Criminal History Record Information” at 28 C.F.R. 20.
- 1.18. ***“Critical Milestone”*** means those milestones critical to the completion of the Services as identified in this Agreement, in any work plan, project plan, statement of work, or other document approved in advance by the Using Agency.
- 1.19. ***“Data Protection Laws”*** means laws, regulations, regulatory requirements, industry self-regulatory standards, and codes of practice in connection with the processing of Personal Information, including those provisions of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. §§1320(d) et seq.) as amended by the Health Information Technology for Economic and Clinical Health Act of 2009 (42 U.S.C. §§ 17921 et seq.) and the Payment Card Industry standards.
- 1.20. ***“Data Security Breach”*** means (a) the loss or misuse (by any means) of any Using Agency Data or other Using Agency Confidential Information; (b) the unauthorized or unlawful access, use, or disclosure of any Using Agency Data or other Using Agency Confidential Information; or (c) any other act or omission that compromises the security, confidentiality, integrity or availability of any Using Agency Data or other Using Agency Confidential Information.
- 1.21. ***“Deliverable”*** has the same meaning as either: (a) “Deliverable” as defined in the County’s Professional Services Agreement, if such document forms the basis of this Agreement; or (b) “Deliverable” as defined in the County’s Instruction to Bidders and General Conditions, if such document forms the basis of this Agreement. In either case, Deliverables includes without limitation Contractor-Provided Equipment, Contractor-Provided Software, Developed Intellectual Property.
- 1.22. ***“Developed Intellectual Property”*** means Intellectual Property as well as any IP Materials conceived, developed, authored or reduced to practice in the course of or in connection with the provision of the Services, including, but not limited to: (a) modifications to, or enhancements (derivative works) of, the Using Agency Intellectual Property or the Using Agency IP Materials; (b) Developed Software; (c) documentation, training materials, or other IP Materials that do not modify or enhance then existing Using Agency IP Materials; and (d) modifications to or enhancements (derivative works) of, Third Party Intellectual Property or related IP Materials to the extent not owned by the licensor of the Third Party Intellectual Property under the terms of the applicable license.
- 1.23. ***“Developed Software”*** any Software conceived, developed, authored or reduced to practice in the course of or in connection with the provision of the Services (including any modifications,

enhancements, patches, upgrades or similar developments).

1.24. ***“Disaster”*** means a sudden, unplanned, calamitous event causing substantial damage or loss as defined or determined by a risk assessment and business impact analysis, and which creates an inability or substantial impairment on the organization’s part to provide critical business functions for a material period of time. This also includes any period when the Using Agency management decides to divert resources from normal production responses and exercises its Disaster Recovery Plan.

1.25. ***“Disaster Recovery Plan”*** means the planned process, and related activities, required to return an IT environment to an acceptable condition of normal business operation following declaration of a Disaster.

1.26. ***“Equipment”*** means the computer, telecommunications, network, storage, and related hardware and peripherals owned or leased by the Using Agency or its Third Party Contractors, or by Contractor or its Subcontractors, and used or supported by Contractor or its Subcontractors, or by the Using Agency or its agents, in connection with the Services.

1.27. ***“Exit Assistance Plan”*** means a detailed plan for the delivery of the Exit Assistance Services.

1.28. ***“Exit Assistance Period”*** has the meaning given in Section 9.2 of this Appendix ‘IT Special Terms and Conditions.’

1.29. ***“Exit Assistance Services”*** means such exit assistance services as are reasonably necessary from Contractor and/or its Subcontractors to enable a complete transition of the affected Services to the Using Agency or the Using Agency’s designee(s), including, but not limited to, all of the services, tasks and functions described in Section 9 of this Appendix ‘IT Special Terms and Conditions.’

1.30. ***“Illicit Code”*** means any hidden files, automatically replicating, transmitting or activating computer program, virus (or other harmful or malicious computer program) or any Equipment-limiting, Software-limiting or Services-limiting function (including, but not limited to, any key, node lock, time-out or similar function), whether implemented by electronic or other means.

1.31. ***“Incident”*** means any event that is not part of the standard operation of a service in the Using Agency IT environment (including an event in respect of the Services or any Equipment or Software) and that causes, or may cause, an interruption to, or a reduction in the quality of, that service. The Using Agency will determine the severity level of each reported Incident.

1.32. ***“Intellectual Property”*** means any inventions, discoveries, designs, processes, software, documentation, reports, and works of authorship, drawings, specifications, formulae, databases, algorithms, models, methods, techniques, technical data, discoveries, know how, trade secrets, and other technical proprietary information and all patents, copyrights, mask works, trademarks, service marks, trade names, service names, industrial designs, brand names, brand marks, trade dress rights, Internet domain name registrations, Internet web sites and corporate names, and applications for the registration or recordation of any of the foregoing. ***“IP Materials”*** means works of authorship, software, documentation, processes, designs, drawings, specifications, formulae, databases, algorithms, models, methods, processes and techniques, technical data, inventions, discoveries, know how, the general format, organization, or structure of any report, document or database, and other technical proprietary information.

1.33. ***“Laws”*** means all United States federal, state and local laws or foreign laws, constitutions,

statutes, codes, rules, regulations, ordinances, executive orders, decrees, edicts of or by any governmental authority having the force of law or any other legal requirement (including common law), including Data Protection Laws and the Cook County Code of Ordinances.

1.34. ***“Open Source Materials”*** means any Software that: (a) contains, or is derived in any manner (in whole or in part) from, any Software that is distributed as free Software, open source Software, shareware (e.g., Linux), or similar licensing or distribution models; and (b) is subject to any agreement with terms requiring that such Software be (i) disclosed or distributed in source code or object code form, (ii) licensed for the purpose of making derivative works, and/or (iii) redistributable. Open Source Materials includes without limitation “open source” code (as defined by the Open Source Initiative) and “free” code (as defined by the Free Software Foundation).

1.35. ***“Party”*** means either County, on behalf of County and its Using Agencies, or Contractor.

1.36. ***“Parties”*** means both County, on behalf of County and its Using Agencies, and Contractor.

1.37. ***“Personal Information”*** means personal data or information that relates to a specific, identifiable, individual person, including Using Agency personnel and individuals about whom the Using Agency, Contractor, Contractor’s Subcontractors or affiliates has or collects financial and other information. For the avoidance of doubt, Personal Information includes the following: (a) any government-issued identification numbers (e.g., Social Security, driver’s license, passport); (b) any financial account information, including account numbers, credit card numbers, debit card numbers, and other Cardholder Data; (c) Criminal Justice Information; (d) Protected Health Information; (e) user name or email address, in combination with a password or security question and answer that would permit access to an account; and (f) any other personal data defined as personally identifiable information under the breach notification laws of the fifty states.

1.38. ***“Problem”*** means the underlying cause of one or more Incidents, including where such cause is unknown or where it is known and a temporary work-around or permanent alternative has been identified.

1.39. ***“Protected Health Information”*** or PHI shall have the same meaning as the term “Protected Health Information” in 45 C.F.R. 160.103.

1.40. ***“Public Record”*** shall have the same meaning as the term “public record” in the Illinois Local Records Act, 50 ILCS 205/1 et seq.

1.41. ***“Required Consent”*** means that consent required to secure any rights of use of or access to any of Using Agency-Provided Equipment, Using Agency-Provided Software, Using Agency Intellectual Property, Using Agency IP Materials, any other Equipment, any other Software whether Third Party Software or otherwise, any other Intellectual Property whether Third Party Intellectual Property or otherwise, any other IP Material, any of which are required by, requested by, used by or accessed by Contractor, its Subcontractors, employees or other agents in connection with the Services.

1.43. ***“Services”*** either: (a) has the same meaning as “Services” as defined in Article 3 of the County’s Professional Services Agreement, if such document forms the basis of this Agreement or (b) collectively means all of Contractor’s services and other acts required in preparing, developing, and tendering the Using Agency’s Deliverables as “Deliverables” is defined in the County’s Instruction to Bidders and General Conditions, if such document forms the basis of this Agreement.

1.44. **“Service Level Agreements”** or **“SLA”** means service level requirement and is a standard for performance of Services, which sets Contractor and Using Agency expectations, and specifies the metrics by which the effectiveness of service activities, functions and processes will be measured, examined, changed and controlled.

1.45. **“Software”** means computer software, including source code, operating system, object, executable or binary code, comments, screens, user interfaces, data structures, data libraries, definition libraries, templates, menus, buttons and icons, and all files, data, materials, manuals, design notes and other items and documentation related thereto or associated therewith.

1.46. **“Third Party”** means a legal entity, company or person that is not a Party to the Agreement and is not a Using Agency, Subcontractor, affiliate of a Party, or other entity, company or person controlled by a Party.

1.47. **“Third Party Intellectual Property”** means all Intellectual Property owned by a Third Party, including Third Party Software.

1.48. **“Third Party Contractor”** means a Third Party that provides the Using Agency with products or services that are related to, or in support of, the Services. Subcontractors of Contractor are not “Third Party Contractors.”

1.49. **“Third Party Software”** means a commercial Software product developed by a Third Party not specifically for or on behalf of the Using Agency. For clarity, custom or proprietary Software, including customizations to Third Party Software, developed by or on behalf of the Using Agency to the Using Agency’s specifications shall not be considered Third Party Software.

1.50. **“Using Agency”** has the same meaning as the term “Using Agency” in the Cook County Procurement Code, located at Chapter 34, Article IV in the Cook County Code of Ordinances as amended, as applied to each department or agency receiving goods, Services or other Deliverables under this Agreement and includes Cook County, a body politic and corporate of the State of Illinois, on behalf of such Using Agency.

1.51. **“Using Agency Confidential Information”** means: (a) all non-public proprietary information of Using Agency that is marked confidential, restricted, proprietary, or with a similar designation; (b) Using Agency Data; and (c) any information that is exempt from public disclosure under the Illinois Freedom of Information Act, 5 ILCS 140/1 et seq. or under the Cook County Code of Ordinances.

1.52. **“Using Agency Data”** means all data, whether Personal Information or other data, provided by the Using Agency to Contractor, provided by Third Parties to Contractor for purposes relating to this Agreement, or otherwise encountered by Contractor for purposes relating to this Agreement, including all data sent to Contractor by the Using Agency and/or stored by Contractor on any media relating to the Agreement, including metadata about such data. To the extent there is any uncertainty as to whether any data constitutes Using Agency Data, the data in question shall be treated as Using Agency Data. Using Agency Data further includes information that is: (a) input, processed or stored by the Using Agency’s IT systems, including any Using Agency-Provided Software; (b) submitted to Contractor or its Subcontractors by any employees, agents, the Using Agency, Third Parties, business partners, and customers in connection with the Services or otherwise; (c) Incident records containing information relating to the Services; (d) Using Agency Intellectual Property and Using Agency IP Materials; (e) any raw data used to generate reports under this Agreement and any data included therein; and (f) Using Agency Confidential Information.

1.53. ***“Using Agency Intellectual Property”*** means all Intellectual Property owned or licensed by the Using Agency, including Developed Intellectual Property.

1.54. ***“Using Agency IP Materials”*** means all IP Materials owned or licensed by the Using Agency.

1.55. ***“Using Agency-Provided Equipment”*** means Equipment provided by or on behalf of Using Agency.

1.56. ***“Using Agency-Provided Software”*** means Software provided by or on behalf of Using Agency.

1.57. ***“WISP”*** means written information security program.

2. Services and Deliverables

2.1. **Approved Facilities.** Contractor will perform Services only within the continental United States and only from locations owned, leased or otherwise utilized by Contractor and its Subcontractors.

2.2. **Licenses and Export Controls.** Contractor will be responsible for obtaining all necessary export authorizations and licenses for export of technical information or data relating to Using Agency Data, Software, Intellectual Property, IP Materials, or otherwise under this Agreement.

2.3. **Required Consents for Assets in Use and Third Party Contracts as of the Effective Date.** Contractor shall be responsible for obtaining all Required Consents relating to this Agreement. If Contractor is unable to obtain a Required Consent, Contractor shall implement, subject to the Using Agency’s prior approval, alternative approaches as necessary to perform the Services. Contractor shall be responsible for and shall pay all costs associated with this section, including any fees or other charges imposed by the applicable Third Parties as a condition or consequence of their consent (*e.g.*, any transfer, upgrade or similar fees). The Using Agency shall cooperate with Contractor and provide Contractor such assistance in this regard as the Contractor may reasonably request.

2.4. **SLAs and Critical Milestones.** Commencing on the Effective Date or as otherwise specified in this Agreement, Contractor shall, as set forth in this Agreement: (a) perform the Services in accordance with SLAs and Critical Milestones; and (b) regularly measure and report on its performance against SLAs and Critical Milestones. Contractor shall maintain all data relating to and supporting the measurement of its performance, including performance against SLAs and Critical Milestones, in sufficient detail to permit a “bottom up” calculation, analysis and reconstruction of performance reports (including all inclusion and exclusion calculations) throughout the term of this Agreement. Such data shall be made available to the Using Agency in an electronic format reasonably acceptable to the Using Agency upon reasonable request and upon the expiration or termination of this Agreement.

2.5. **Default SLAs, Critical Milestones and Fee Reductions.** Unless otherwise explicitly specified in this Agreement, the Contractor’s SLAs, SLA targets, and Critical Milestones shall be those that the Using Agency recognizes as commonly accepted “industry best practices” for Services of similar cost, size, and criticality. For example and without limitation, such SLAs include availability and performance Contractor-Provided Software and hosting-related Services, on-time delivery of Deliverables, response and resolution times of Contractor’s service desk. For example and without

limitation, such Critical Milestones include significant events in projects such as completion of major Deliverables. Unless otherwise specified in this Agreement, Contractor shall proportionately reduce fees for failing to perform the Services in accordance with applicable SLAs and for failing to timely achieve Critical Milestones, and the Using Agency may withhold that amount of fee reduction from any outstanding Contractor invoice. Except as expressly allowed under this Agreement, any such fee reduction accompanying a failure to meet applicable SLAs or Critical Milestones shall not be the Using Agency's exclusive remedy and shall not preclude the Using Agency from seeking other remedies available to it for a material breach of this Agreement.

2.6. Standards and Procedures Manual. Contractor will prepare, update, and maintain a manual ("Standards and Procedures Manual") subject to the Using Agency's review and approval that shall: (a) be based upon ITIL processes and procedures; (b) conform to the Using Agency's standard operating procedures (c) be suitable to assist the Using Agency and the Using Agency's auditors in verifying and auditing the Contractor's performance of the Services; and (d) detail the operational and management processes by which Contractor will perform the Services under this Agreement, including to the extent applicable, processes relating to: (i) Change Management and Change control; (ii) Incident management; (iii) Problem management; (iv) configuration management; (v) backup and restore; (vi) capacity management and full utilization of resources; (vii) project management; (viii) management information; (ix) security processes; (x) Contractor's Business Continuity Plan; (xi) Contractor's Disaster Recovery Plan; and (xi) administration, including invoicing. Where this Agreement assumes that the Using Agency will provide Tier 1 help desk support, the Standards and Procedures Manual shall also include sufficient help desk scripts for the Using Agency to provide such support. Contractor will perform the Services in accordance with the Standards and Procedures Manual; *provided, however*, that the provisions of the Standards and Procedures Manual shall never supersede the provisions of this Agreement.

2.7. Project Management Methodology. Contractor shall perform the Services in accordance with an industry-recognized project management methodology and procedures, subject to Using Agency approval. Contractor shall comply with the Using Agency's procedures for tracking progress and documents for the duration of the Agreement, including the submission of weekly or monthly status reports to the Using Agency as the Using Agency may require.

2.8. Change Management Procedures. Contractor shall utilize Change Management procedures, subject to Using Agency approval, that conform to ITIL/ITSM to manage, track and report on Changes relating to the Services, including procedures for scheduling maintenance, patching, replacement of assets, and other matters required for proper management of the Services. No Change will be made without the Using Agency's prior written consent (which may be given or withheld in the Using Agency's sole discretion), unless such Change: (a) has no impact on the Services being provided by Contractor; (b) has no impact on the security of the Using Agency Data and the Using Agency systems; and (c) causes no increase in any fees under this Agreement or the Using Agency's retained costs.

2.9. Resources Necessary for Services. Except as set forth in this Agreement, Contractor shall provide and be financially responsible for all Equipment, Software, materials, facilities, systems and other resources needed to perform the Services in accordance with the Agreement.

2.10. Using Agency Resources. Except as explicitly allowed under this Agreement, Contractor shall not use, nor permit any Subcontractor, employee, agent, or other Third Party to use any Using Agency-Provided Equipment, Using Agency-Provided Software, Using Agency facilities, or any other Equipment, Software, materials, facilities, systems or other resources that the Using Agency provides or otherwise makes available under this Agreement for any purpose other than the performance of the Services; and Contractor

shall do so only upon prior written approval of the Using Agency. Contractor shall not purport to, pledge or charge by way of security any of the aforementioned. Contractor shall keep any Equipment owned or leased by the Using Agency that is under Contractor's or a Contractor Subcontractor's control, secure and, for any such Equipment that is not located at the Using Agency facilities, such Equipment shall be clearly identified as the Using Agency's and separable from Contractor's and Third Parties' property.

2.11. Maintenance of Assets. Contractor shall maintain all Equipment, Software, materials, systems, and other resources utilized predominately or exclusively for performing Services in good condition, less ordinary wear and tear, and in such locations and configurations as to be readily identifiable.

2.12. Service Compatibility. To the extent necessary to provide the Services, Contractor shall ensure that the Services, Contractor-Provided Equipment and Contractor-Provided Software (collectively, the "Contractor Resources") are interoperable with the Using Agency-Provided Equipment, Using Agency-Provided Software and with the Using Agency's other Assets, at no cost beyond that specified in this Agreement and without adversely affecting any systems or services retained by the Using Agency or its Third Party Contractors. In the event of any Problem related to service compatibility where it is not known whether the Problem is caused by Contractor's Assets or by Using Agency's Assets, Contractor shall be responsible for correcting the Problem except to the extent that Contractor can demonstrate, to the Using Agency's satisfaction, that the cause was not due to Contractor Resources or to Contractor's action or inaction.

2.13. Cooperation with Using Agency's Third Party Contractors. Contractor shall cooperate with all Third Party Contractors to coordinate its performance of the Services with the services and systems of such Third Party Contractors. Subject to reasonable confidentiality requirements, such cooperation shall include providing: (a) applicable written information, standards and policies concerning any or all of the systems, data, computing environment, and technology direction used in performing the Services so that the goods and services provided by the Third Party Contractor may work in conjunction with or be integrated with the Services; (b) assistance and support services to such Third Party Contractors; (c) Contractor's quality assurance, its development and performance acceptance testing and the applicable requirements of any necessary interfaces for the Third Party Contractor's work product; (d) applicable written requirements of any necessary modifications to the systems or computing environment; and (e) access to and use of the Contractor's Assets as mutually agreed upon by the Using Agency and Contractor (such agreement not to be unreasonably withheld or delayed) and subject to the Third Party Contractor's agreement to comply with Contractor's applicable standard security policies.

2.14. Procurement Assistance. At any time during the Agreement, Contractor shall, as requested by the Using Agency, reasonably cooperate and assist the Using Agency with any Using Agency procurement relating to any of the Services or replacing the Services, including: (a) providing information, reports and data for use in the Using Agency's procurement or transition to a subsequent Third Party Contractor; (b) answering Third Parties' and Using Agency's questions regarding the procurement and Services transition; and (c) allowing Third Parties participating in the Using Agency's procurement to perform reasonable, non-disruptive due diligence activities in respect of the relevant Services, including providing reasonable access to Key Personnel.

3. Warranties

3.1. Compliance with Law and Regulations. Contractor represents and warrants that it shall perform its obligations under this Agreement in accordance with all Laws applicable to Contractor and its business, including Laws applicable to the manner in which the Services are performed, including any

changes in such Laws. With respect to laws governing data security and privacy, the term ‘Contractor Laws’ shall include any Laws that would be applicable to Contractor if it, rather than the Using Agency, were the owner or data controller of any of the Using Agency Data in its possession or under its control in connection with the Services. Contractor also represents and warrants that it shall identify, obtain, keep current, and provide for Contractor’s inspection, all necessary licenses, approvals, permits, authorizations, visas and the like as may be required from time to time under Contractor Laws for Contractor to perform the Services.

3.2. Non-Infringement. Contractor represents and warrants that it shall perform its responsibilities under this Agreement in a manner that does not infringe any patent, copyright, trademark, trade secret or other proprietary rights of any Third Party.

3.3. Contractor Materials and Third Party Intellectual Property. Contractor represents and warrants that it owns, or is authorized to use, all Contractor Intellectual Property, Contractor IP Materials and Contractor-provided Third Party Intellectual Property.

3.4. Developed Software. Contractor represents and warrants that all Developed Software shall be free from material errors in operation and performance, shall comply with the applicable documentation and specifications in all material respects, for twelve (12) months after the installation, testing and acceptance of such Developed Software by the Using Agency; provided, however, for Developed Software that executes on a monthly or less frequent basis (e.g., quarterly or annual cycle), such warranty period will commence on the date of first execution of such Software. Any repairs made to Developed Software pursuant to this Section shall receive a new twelve (12) month warranty period in accordance with the terms of this Section.

3.5. No Open Source. Contractor represents and warrants that Contractor has not (i) incorporated Open Source Materials into, or combined Open Source Materials with, the Deliverables or Software, (ii) distributed Open Source Materials in conjunction with any Deliverables or Software, or (iii) used Open Source Materials, in such a way that, with respect to the foregoing (i), (ii), or (iii), creates obligations for the Contractor with respect to any material Deliverables or grant, or purport to grant, to any Third Party, any rights or immunities under any material Deliverables (including, but not limited to, using any Open Source Materials that require, as a condition of use, modification and/or distribution of such Open Source Materials that other material Software included in Deliverables incorporated into, derived from or distributed with such Open Source Materials be (A) disclosed or distributed in source code form, (B) be licensed for the purpose of making derivative works, or (C) be redistributable at no charge).

3.6. Access to Using Agency Data. Contractor represents and warrants that Contractor has not and will not prevent, or reasonably fail to allow, for any reason including without limitation late payment or otherwise, the Using Agency’s access to and retrieval of Using Agency Data. Contractor acknowledges that Using Agency Data may be Public Records and that any person who knowingly, without lawful authority and with the intent to defraud any party, public officer, or entity, alters, destroys, defaces, removes, or conceals any Public Record commits a Class 4 felony.

3.7. Viruses. Contractor represents and warrants that it has not knowingly provided, and will not knowingly provide, to the Using Agency in connection with the Services, any Software that uses Illicit Code. Contractor represents and warrants that it has not and will not introduce, invoke or cause to be invoked such Illicit Code in any Using Agency IT environment at any time, including upon expiration or termination of this Agreement for any reason, without the Using Agency’s prior written consent. If Contractor discovers that Illicit Code has been introduced into Software residing on Equipment hosted or supported by Contractor, Contractor shall, at no additional charge, (a) immediately undertake to remove such Illicit Code, (b) promptly notify the Using Agency in writing of the introduction, and (c) use reasonable efforts to correct and repair

any damage to Using Agency Data or Software caused by such Illicit Code and otherwise assist the Using Agency in mitigating such damage and restoring any affected Service, Software or Equipment.

3.8. Resale of Equipment and Software. If Contractor resells to the Using Agency any Equipment or Software that Contractor purchased from a Third Party, then Contractor, to the extent it is legally able to do so, shall pass through any such Third Party warranties to the Using Agency and reasonably cooperate in enforcing them. Such warranty pass-through will not relieve Contractor from its warranty obligations set forth in this Section.

3.9. Data Security. Contractor warrants and represents that (i) the performance of the Services shall not permit any unauthorized access to or cause any loss or damage to Using Agency Data, Using Agency Intellectual Property, or other Using Agency Confidential Information; and (ii) it complies and shall comply with all Using Agency security policies in place from time to time during the term of this Agreement.

4. Intellectual Property

4.1. Using Agency Intellectual Property. The Using Agency retains all right, title and interest in and to all Using Agency Intellectual Property and Using Agency IP Materials. To the extent the Using Agency may grant such license, Contractor is granted a worldwide, fully paid-up, nonexclusive license during the term of this Agreement to use, copy, maintain, modify, enhance and create derivative works of the Using Agency Intellectual Property and Using Agency IP Materials that are necessary for performing the Services, and that are explicitly identified in writing by the Using Agency's Chief Information Officer, for the sole purpose of performing the Services pursuant to this Agreement. Contractor shall not be permitted to use any of the Using Agency Intellectual Property or Using Agency IP Materials for the benefit of any entities other than the Using Agency. Contractor shall cease all use of the Using Agency Intellectual Property and Using Agency IP Materials upon expiration or termination of this Agreement. Upon expiration or termination of this Agreement or relevant Services under this Agreement, Contractor shall return to the Using Agency all the Using Agency Intellectual Property, Using Agency IP Materials and copies thereof possessed by Contractor.

4.2. Developed Intellectual Property. As between the Parties, the Using Agency shall have all right, title and interest in all Developed Intellectual Property. Contractor hereby irrevocably and unconditionally assigns, transfers and conveys to the Using Agency without further consideration all of its right, title and interest in such Developed Intellectual Property, including all rights of patent, copyright, trade secret or other proprietary rights in such materials, which assignment shall be effective as of the creation of such works without need for any further documentation or action on the part of the Parties. Contractor agrees to execute any documents or take any other actions as may reasonably be necessary, or as the Using Agency may reasonably request, to perfect the Using Agency's ownership of any such Developed Intellectual Property. Contractor shall secure compliance with this Section by any personnel, employees, contractors or other agents of Contractor and its Subcontractors involved directly or indirectly in the performance of Services under this Agreement.

4.3. Contractor Intellectual Property. Contractor retains all right, title and interest in and to Contractor Intellectual Property and Contractor IP Materials that Contractor developed before or independently of this Agreement. Contractor grants to the Using Agency, a fully-paid, royalty-free, non-exclusive, non-transferable, worldwide, irrevocable, perpetual, assignable license to make, have made, use, reproduce, distribute, modify, publicly display, publicly perform, digitally perform, transmit, copy, and create derivative works based upon Contractor Intellectual Property and Contractor IP Materials, in any media now known or hereafter known, to the extent the same are embodied in the Services and Deliverables,

or otherwise required to exploit the Services or Deliverables. During the term of this Agreement and immediately upon any expiration or termination thereof for any reason, Contractor will provide to the Using Agency the most current copies of any Contractor IP Materials to which the Using Agency has rights pursuant to the foregoing, including any related documentation. Contractor bears the burden to prove that Intellectual Property and IP Materials related to this Agreement were not created under this Agreement.

4.4. Third Party Intellectual Property. Contractor shall not introduce into the Using Agency's environment any Third Party Intellectual Property or otherwise use such Third Party Intellectual Property to perform the Services without first obtaining the prior written consent from the Using Agency's Chief Information Officer, which the Using Agency may give or withhold in its sole discretion. A decision by the Using Agency to withhold its consent shall not relieve Contractor of any obligation to perform the Services.

4.5. Residual Knowledge. Nothing contained in this Agreement shall restrict either Contractor or Using Agency from the use of any ideas, concepts, know-how, methodologies, processes, technologies, algorithms or techniques relating to the Services which either Contractor or Using Agency, individually or jointly, develops or discloses under this Agreement, provided that in doing so Contractor or Using Agency does not breach its respective obligations under Section 5 relating to confidentiality and non-disclosure and does not infringe the Intellectual Property rights of the other or Third Parties who have licensed or provided materials to the other. Except for the license rights contained under Section 4, neither this Agreement nor any disclosure made hereunder grants any license to either Contractor or Using Agency under any Intellectual Property rights of the other.

4.6. Software Licenses. This Agreement contains all terms and conditions relating to all licenses in Contractor-Provided Software and Contractor IP Materials. Except as explicitly set forth elsewhere in this Agreement, all licenses that Contractor grants in Contractor-Provided Software include the right of use by Third Party Contractors for the benefit of the Using Agency, the right to make backup copies for backup purposes or as may be required by the Using Agency's Business Continuity Plan or Disaster Recovery Plan, the right to reasonably approve the procedures by which Contractor may audit the use of license entitlements, and the right to give reasonable approval before Contractor changes Contractor-Provided Software in a manner that materially and negatively impacts the Using Agency.

5. Using Agency Data and Confidentiality

5.1. Property of Using Agency. All Using Agency Confidential Information, including without limitation Using Agency Data, shall be and remain the sole property of the Using Agency. Contractor shall not utilize the Using Agency Data or any other Using Agency Confidential Information for any purpose other than that of performing the Services under this Agreement. Contractor shall not, and Contractor shall ensure that its Subcontractors, its employees, or agents do not, possess or assert any lien or other right against or to the Using Agency Data or any other Using Agency Confidential Information. Without the Using Agency's express written permission, which the Using Agency may give or withhold in its sole discretion, no Using Agency Data nor any other Using Agency Confidential Information, or any part thereof, shall be disclosed, shared, sold, assigned, leased, destroyed, altered, withheld, or otherwise restricted of by Contractor or commercially exploited by or on behalf of Contractor, its employees, Subcontractors or agents.

5.2. Acknowledgment of Importance of Using Agency Confidential Information. Contractor acknowledges the importance of Using Agency Confidential Information, including without limitation Using Agency Data, to the Using Agency and, where applicable, Third Party proprietors of such information, and recognizes that the Using Agency and/or Third Party proprietors may suffer irreparable harm or loss in the event of such information being disclosed or used otherwise than in accordance with this Agreement.

5.3. Return of Using Agency Data and Other Using Agency Confidential Information. Upon the Using Agency's request, at any time during this Agreement or at termination or expiration of this Agreement, Contractor shall promptly return any and all requested Using Agency Data and all other requested Using Agency Confidential Information to the Using Agency or its designee in such a format as the Using Agency may reasonably request. Contractor shall also provide sufficient information requested by the Using Agency about the format and structure of the Using Agency Data to enable such data to be used in substantially the manner in which Contractor utilized such data. Also upon Using Agency's request, in lieu of return or in addition to return, Contractor shall destroy Using Agency Data and other Using Agency Confidential Information, sanitize any media upon which such the aforementioned resided using a process that meets or exceeds DoD 5220.28-M 3-pass specifications, and provide documentation of same within 10 days of completion, all in compliance with Using Agency's policies and procedures as updated. All other materials which contain Using Agency Data and other Using Agency Confidential Information shall be physically destroyed and shredded in accordance to NIST Special Publication 800-88; and upon Using Agency request, Contractor shall provide Using Agency with a certificate of destruction in compliance with NIST Special Publication 800-88. Contractor shall be relieved from its obligation to perform any Service to the extent the return of any Using Agency Data or other Using Agency Confidential Information at the Using Agency's request under this Section materially impacts Contractor's ability to perform such Service; provided, that Contractor gives the Using Agency notice of the impact of the return and continues to use reasonable efforts to perform.

5.4. Public Records. Contractor will adhere to all Laws governing Public Records located at 50 ILCS 205/1 et seq. and at 44 Ill. Admin. Code 4500.10 et seq. Specifically, and without limitation, Contractor shall: (a) store Using Agency Data in such a way that each record is individually accessible for the length of the Using Agency's scheduled retention; (b) retain a minimum of two total copies of all Using Agency Data; (c) retain Using Agency Data according to industry best practices for geographic redundancy, such as NIST Special Publication 800-34 as revised; (d) store and access Using Agency Data in a manner allowing individual records to maintain their relationships with one another; (e) capture relevant structural, descriptive, and administrative metadata to Using Agency Data at the time a record is created or enters the control of Contractor or its Subcontractors.

5.4. Disclosure Required by Law, Regulation or Court Order. In the event that Contractor is required to disclose Using Agency Data or other Using Agency Confidential Information in accordance with a requirement or request by operation of Law, regulation or court order, Contractor shall, except to the extent prohibited by law: (a) advise the Using Agency thereof prior to disclosure; (b) take such steps to limit the extent of the disclosure to the extent lawful and reasonably practical; (c) afford the Using Agency a reasonable opportunity to intervene in the proceedings; and (d) comply with the Using Agency's requests as to the manner and terms of any such disclosure.

5.5. Loss of Using Agency Confidential Information. Without limiting any rights and responsibilities under Section 7 of these IT Special Conditions, in the event of any disclosure or loss of, or inability to account for, any Using Agency Confidential Information, Contractor shall promptly, at its own expense: (a) notify the Using Agency in writing; (b) take such actions as may be necessary or reasonably requested by the Using Agency to minimize the violation; and (c) cooperate in all reasonable respects with the Using Agency to minimize the violation and any damage resulting therefrom.

5.6. Undertakings With Respect To Personnel. Contractor acknowledges and agrees that it is responsible for the maintenance of the confidentiality of Using Agency Data and other Using Agency Confidential Information by Contractor Personnel. Without limiting the generality of the foregoing, Contractor shall undertake to inform all Contractor Personnel of Contractor's obligations with respect to

Using Agency Data and other Using Agency Confidential Information and shall undertake to ensure that all Contractor Personnel comply with Contractor's obligations with respect to same.

5.7. Background Checks of Contractor Personnel. Whenever the Using Agency deems it reasonably necessary for security reasons, the Using Agency or its designee may conduct, at its expense, criminal and driver history background checks of Contractor Personnel. Contractor and its Subcontractors shall immediately reassign any individual who, in the opinion of the Using Agency, does not pass the background check.

5.8 Contractor Confidential Information. Using Agency shall use at least the same degree of care to prevent disclosing Contractor Confidential Information to Third Parties as Using Agency employs to avoid unauthorized disclosure, publication or dissemination of its Using Agency Confidential Information of like character.

6. Data Security and Privacy

6.1. General Requirement of Confidentiality and Security. It shall be Contractor's obligation to maintain the confidentiality and security of all Using Agency Confidential Information, including without limitation Using Agency Data, in connection with the performance of the Services. Without limiting Contractor's other obligations under this Agreement, Contractor shall implement and/or use network management and maintenance applications and tools and appropriate fraud prevention and detection and encryption technologies to protect the aforementioned; provided that Contractor shall, at a minimum, encrypt all Personal Information in-transit and at-rest. Contractor shall perform all Services utilizing security technologies and techniques and in accordance with industry leading practices and the Using Agency's security policies, procedures and other requirements made available to Contractor in writing, including those relating to the prevention and detection of fraud or other inappropriate use or access of systems and networks.

6.2. General Compliance. Contractor shall comply with all applicable Laws, regulatory requirements and codes of practice in connection with all capturing, processing, storing and disposing of Personal Information by Contractor pursuant to its obligations under this Agreement and applicable Data Protection Laws and shall not do, or cause or permit to be done, anything that may cause or otherwise result in a breach by the Using Agency of the same. Contractor and all Contractor Personnel shall comply with all the Using Agency policies and procedures regarding data access, privacy and security.

6.3. Security. Contractor shall establish and maintain reasonable and appropriate physical, logical, and administrative safeguards to preserve the security and confidentiality of the Using Agency Data and other Using Agency Confidential Information and to protect same against unauthorized or unlawful disclosure, access or processing, accidental loss, destruction or damage. Such safeguards shall be deemed reasonable and appropriate if established and maintained with the more rigorous of: (a) the Using Agency Policies as updated; (b) the security standards employed by Contractor with respect to the protection of its confidential information and trade secrets as updated; (c) security standards provided by Contractor to its other customers at no additional cost to such customers, as updated; or (d) compliance with the then-current NIST 800-series enterprise standards and successors thereto or an enterprise level equivalent, generally accepted, industry-standard security standards series.

6.4. Written Information Security Program. Contractor shall establish and maintain a WISP designed to preserve the security and confidentiality of the Using Agency Data and other Using Agency Confidential Information. Contractor's WISP shall include Data Breach procedures and annual Data Breach response exercises. Contractor's WISP shall be reasonably detailed and shall be subject to the Using

Agency's reasonable approval.

6.5. Contractor Personnel. Contractor will oblige its Contractor Personnel to comply with applicable Data Protection Laws and to undertake only to collect, process or use any Using Agency Data, Using Agency Intellectual Property, Using Agency Confidential Information, or Personal Information received from or on behalf of the Using Agency for purposes of, and necessary to, performing the Services and not to make the aforementioned available to any Third Parties except as specifically authorized hereunder. Contractor shall ensure that, prior to performing any Services or accessing any Using Agency Data or other Using Agency Confidential Information, all Contractor Personnel who may have access to the aforementioned shall have executed agreements concerning access protection and data/software security consistent with this Agreement.

6.6. Information Access. Contractor shall not attempt to or permit access to any Using Agency Data or other Using Agency Confidential Information by any unauthorized individual or entity. Contractor shall provide each of the Contractor Personnel, Subcontractors and agents only such access as is minimally necessary for such persons/entities to perform the tasks and functions for which they are responsible. Contractor shall, upon request from the Using Agency, provide the Using Agency with an updated list of those Contractor Personnel, Subcontractors and agents having access to Using Agency Data and other Using Agency Confidential Information and the level of such access. Contractor shall maintain written policies that include auditing access levels and terminating access rights for off-boarded Contractor Personnel, Subcontractors and agents.

6.7. Protected Health Information. If Contractor will have access to Personal Health Information in connection with the performance of the Services, Contractor shall execute a Business Associate Agreement in a form provided by the Using Agency.

6.8. Criminal Justice Information. If Contractor will have access to Criminal Justice Information in connection with the performance of the Services, Contractor shall execute an addendum to this Agreement governing the Contractor's access to such Criminal Justice Information in a form provided by the Using Agency.

6.9. Cardholder Data. If Contractor will have access to Cardholder Data in connection with the performance of the Services, no less than annually, Contractor shall tender to Using Agency a current attestation of compliance signed by a Qualified Security Assessor certified by the Payment Card Industry.

6.10. Encryption Requirement. Contractor shall encrypt all Personal Information and all other Using Agency Confidential Information the disclosure of which would reasonably threaten the confidentiality and security of Using Agency Data. Contractor shall encrypt the aforementioned in motion, at rest and in use in a manner that, at a minimum, adheres to NIST SP 800-111, NIST SP 800-52, NIST SP 800-77 and NIST SP 800-113 encryption standards. Contractor shall not deviate from this encryption requirement without the advance, written approval of the Using Agency's Information Security Office.

6.11. Using Agency Security. Contractor shall notify the Using Agency if it becomes aware of any Using Agency security practices or procedures (or any lack thereof) that Contractor believes do not comport with generally accepted security policies or procedures.

6.12. Contractor as a Data Processor. Contractor understands and acknowledges that, to the extent that performance of its obligations hereunder involves or necessitates the processing of Personal Information, it shall act only on instructions and directions from the Using Agency; *provided, however*, that Contractor shall notify the Using Agency if it receives instructions or directions from the Using Agency that

Contractor believes do not comport with generally accepted security policies or procedures and the Using Agency shall determine whether to modify such instructions or have Contractor comply with such instructions unchanged.

6.13. Data Subject Right of Access and Rectification. If the Using Agency is required to provide or rectify information regarding an individual's Personal Information, Contractor will reasonably cooperate with the Using Agency to the full extent necessary to comply with Data Protection Laws. If a request by a data subject is made directly to Contractor, Contractor shall notify the Using Agency of such request as soon as reasonably practicable.

6.14. Security, Privacy and Data Minimization in Software Development Life Cycle. Contractor shall implement an industry-recognized procedure that addresses the security and privacy of Personal Information as part of the software development life cycle in connection with the performance of the Services. Contractor shall implement procedures to minimize the collection of Personal Information and shall, subject to Using Agency's written request to the contrary, minimize the collection of Personal Information.

6.15. Advertising and Sale of Using Agency Data. Nothing in this Agreement shall be construed to limit or prohibit a Using Agency's right to advertise, sell or otherwise distribute Using Agency Data as permitted by the Cook County Code of Ordinances.

7. Data Security Breach

7.1. Notice to Using Agency. Contractor shall provide to the Using Agency written notice of such Data Security Breach promptly following, and in no event later than one (1) business day following, the discovery or suspicion of the occurrence of a Data Security Breach. Such notice shall summarize in reasonable detail the nature of the Using Agency Data that may have been exposed, and, if applicable, any persons whose Personal Information may have been affected, or exposed by such Data Security Breach. Contractor shall not make any public announcements relating to such Data Security Breach without the Using Agency's prior written approval.

7.2. Data Breach Responsibilities. If Contractor knows or has reason to know that a Data Security Breach has occurred (or potentially has occurred), Contractor shall: (a) reasonably cooperate with the Using Agency in connection with the investigation of known and suspected Data Security Breaches; (b) perform any corrective actions that are within the scope of the Services; and (c) at the request and under the direction of the Using Agency, take any all other remedial actions that the Using Agency deems necessary or appropriate, including without limitation, providing notice to all persons whose Personal Information may have been affected or exposed by such Data Security Breach, whether or not such notice is required by Law.

7.3. Data Breach Exercises. Contractor shall conduct annual Data Breach exercises. Upon Using Agency request, Contractor shall coordinate its exercises with the Using Agency.

7.4. Costs. The costs incurred in connection with Contractor's obligations set forth in Section 7 or Using Agency's obligations under relevant Data Security Laws shall be the responsibility of the Party whose acts or omissions caused or resulted in the Data Security Breach and may include without limitation: (a) the development and delivery of legal notices or reports required by Law, including research and analysis to determine whether such notices or reports may be required; (b) examination and repair of Using Agency Data that may have been altered or damaged in connection with the Data Security Breach, (c) containment, elimination and remediation of the Data Security Breach, and (d) implementation of new or additional

security measures reasonably necessary to prevent additional Data Security Breaches; (e) providing notice to all persons whose Personal Information may have been affected or exposed by such Data Security Breach, whether or required by Law; (f) the establishment of a toll-free telephone number, email address, and staffing of corresponding communications center where affected persons may receive information relating to the Data Security Breach; (g) the provision of one (1) year of credit monitoring/repair and/or identity restoration/insurance for affected persons.

8. Audit Rights

8.1. Generally. Contractor and its Subcontractors shall provide access to any records, facilities, personnel, and systems relating to the Services, at any time during standard business hours, to the Using Agency and its internal or external auditors, inspectors and regulators in order to audit, inspect, examine, test, and verify: (a) the availability, integrity and confidentiality of Using Agency Data and examine the systems that process, store, support and transmit Using Agency Data; (b) controls placed in operation by Contractor and its Subcontractors relating to Using Agency Data and any Services; (c) Contractor's disaster recovery and backup/recovery processes and procedures; and (d) Contractor's performance of the Services in accordance with the Agreement. The aforementioned Using Agency audit rights include the Using Agency's right to verify or conduct its own SOC 2 audits.

8.2. Security Audits. Contractor shall perform, at its sole cost and expense, a security audit no less frequently than every twelve (12) months. The security audit shall test Contractor's compliance with security standards and procedures set forth in: (a) this Agreement, (b) the Standards and Procedures Manual, and (c) any security standards and procedures otherwise agreed to by the Parties.

8.3. Service Organization Control (SOC 2), Type II Audits. Contractor shall, at least once annually in the fourth (4th) calendar quarter and at its sole cost and expense, provide to the Using Agency and its auditors a Service Organization Control (SOC 2), Type II report for all locations at which the Using Agency Data is processed or stored.

8.4. Audits Conducted by Contractor. Contractor promptly shall make available to the Using Agency the results of any reviews or audits conducted by Contractor and its Subcontractors, agents or representatives (including internal and external auditors), including SOC 2 audits, relating to Contractor's and its Subcontractors' operating practices and procedures to the extent relevant to the Services or any of Contractor's obligations under the Agreement. To the extent that the results of any such audits reveal deficiencies or issues that impact the Using Agency or the Services, Contractor shall provide the Using Agency with such results promptly following completion thereof.

8.5. Internal Controls. Contractor shall notify the Using Agency prior to modifying any of its internal controls that impact the Using Agency, the Services and/or Using Agency Data and shall demonstrate compliance with this Agreement.

8.6. Subcontractor Agreements. Contractor shall ensure that all agreements with its Subcontractors performing Services under this Agreement contain terms and conditions consistent with the Using Agency's audit rights.

9. Right to Exit Assistance

9.1. Payment for Exit Assistance Services. Exit Assistance Services shall be deemed a part of the Services and included within the Contractor's fees under this Agreement, except as otherwise detailed

in this Agreement.

9.2. General. Upon Using Agency's request in relation to any termination, regardless of reason, or expiration of the Agreement, in whole or in part, Contractor shall provide the Using Agency and each of its designees Exit Assistance Services. During the Exit Assistance Period, Contractor shall continue to perform the terminated Services except as approved by the Using Agency and included in the Exit Assistance Plan. Contractor's obligation to provide the Exit Assistance Services shall not cease until the Services have been completely transitioned to the Using Agency or the Using Agency's designee(s) to the Using Agency's satisfaction.

9.3. Exit Assistance Period. Contractor shall: (a) commence providing Exit Assistance Services at the Using Agency's request (i) up to six (6) months prior to the expiration of the Agreement, or (ii) in the event of termination of the Agreement or any Services hereunder, promptly following receipt of notice of termination from the Party giving such notice (such date notice is received, the "Termination Notice Date"), and (b) continue to provide the Exit Assistance Services through the effective date of termination or expiration of the Agreement or the applicable terminated Services (as applicable, the "Termination Date") (such period, the "Exit Assistance Period"). At the Using Agency's option, the Exit Assistance Period may be extended for a period of up to twelve (12) months after the Termination Date. The Using Agency shall provide notice regarding its request for Exit Assistance Services at least sixty (60) days prior to the date upon which the Using Agency requests that Contractor commence Exit Assistance Services unless such time is not practicable given the cause of termination.

9.4. Manner of Exit Assistance Services. Contractor shall perform the Exit Assistance Services in a manner that, to the extent the same is within the reasonable control of Contractor: (a) is in accordance with the Using Agency's reasonable direction; (b) is in cooperation with, and causes its Subcontractors to cooperate with, the Using Agency and the Using Agency's designee(s); (c) supports the efficient and orderly transfer of the terminated Services to the Using Agency; (d) minimizes any impact on the Using Agency's operations; (e) minimizes any internal and Third Party costs incurred by the Using Agency and the Using Agency's designee(s); and (f) minimizes any disruption or deterioration of the terminated Services. Exit Assistance Plan. Contractor shall develop and provide to the Using Agency, subject to the Using Agency's approval and authorization to proceed, an Exit Assistance Plan that shall: (a) describe responsibilities and actions to be taken by Contractor in performing the Exit Assistance Services; (b) describe in detail any Using Agency Responsibilities which are necessary for Contractor to perform the Exit Assistance Services; (c) describe how any transfer of Assets and any novation, assignment or transfer of contracts will be achieved during the Exit Assistance Period; (d) detail the return, and schedule for return, of Using Agency Data and other Using Agency-specific information to be provided; (e) set out the timetable for the transfer of each element of the terminated Services (including key milestones to track the progress); (f) identify a responsible party for each service, task and responsibility to be performed under the Exit Assistance Plan; and (g) specify reasonable acceptance criteria and testing procedures to confirm whether the transfer of the terminated Services has been successfully completed. Following the Using Agency's approval of, and authorization to proceed with the final Exit Assistance Plan, Contractor will perform the Exit Assistance Services in accordance with the Exit Assistance Plan.

9.6. Exit Assistance Management. Within the first thirty (30) days of the Exit Assistance Period, Contractor will appoint a senior project manager to be responsible for, and Contractor's primary point of contact for, the overall performance of the Exit Assistance Services. Upon Using Agency request, Contractor will provide individuals with the required expertise to perform Exit Assistance Services, even if those individuals are not currently performing Services. Contractor will promptly escalate to the Using Agency any failures (or potential failures) regarding the Exit Assistance Services. Contractor will meet weekly with the Using Agency and provide weekly reports describing: the progress of the Exit Assistance Services

against the Exit Assistance Plan; any risks encountered during the performance of the Exit Assistance Services; and proposed steps to mitigate such risks. The Using Agency may appoint, during the Exit Assistance Period, a Using Agency designee to be the Using Agency's primary point of contact and/or to operationally manage Contractor during the Exit Assistance Period.

9.7. Removal of Contractor Materials. Contractor shall be responsible at its own expense for de-installation and removal from the Using Agency Facilities any Equipment owned or leased by Contractor that is not being transferred to the Using Agency under the Agreement subject to the Using Agency's reasonable procedures and in a manner that minimizes the adverse impact on the Using Agency. Prior to removing any documents, equipment, software or other material from any Using Agency Facility, Contractor shall provide the Using Agency with reasonable prior written notice identifying the property it intends to remove. Such identification shall be in sufficient detail to apprise the Using Agency of the nature and ownership of such property.

9.8. Using Agency-specific Information. Upon Using Agency's request, Contractor will specifically provide to the Using Agency the following Using Agency Data relating to the Services: (a) SLA statistics, reports and associated raw data; (b) operational logs; (c) the Standards and Procedures Manual; (d) Incident and Problem logs for at least the previous two (2) years; (e) security features; (f) passwords and password control policies; (g) identification of work planned or in progress as of the Termination Date, including the current status of such work and projects; and (h) any other information relating to the Services or the Using Agency's IT or operating environment which would be required by a reasonably skilled and experienced Contractor of services to assume and to continue to perform the Services following the Termination Date without disruption or deterioration. This section shall not limit any other rights and duties relating to Using Agency Data.

9.9. Subcontractors and Third Party Contracts. For each contract for which Using Agency has an option to novate or transfer, Contractor will supply the following information upon Using Agency's request: (a) description of the goods or service being provided under the contract; (b) whether the contract exclusively relates to the Services; (c) whether the contract can be assigned, novated or otherwise transferred to the Using Agency or its designee and any restrictions or costs associated with such a transfer; (d) the licenses, rights or permissions granted pursuant to the contract by the Third Party; (e) amounts payable pursuant to the terms of such contract; (f) the remaining term of the contract and termination rights; and (g) contact details of the Third Party. Contractor's agreements with Third Parties that predominantly or exclusively relate to this Agreement shall not include any terms that would restrict such Third Parties from entering into agreements with the Using Agency or its designees as provided herein.

9.10. Knowledge Transfer. As part of the Exit Assistance Services and upon Using Agency's reasonable request, Contractor will provide knowledge transfer services to the Using Agency or the Using Agency's designee to allow the Using Agency or such designee to fully assume, become self-reliant with respect to, and continue without interruption, the provision of the terminated Services. Contractor shall: allow personnel of the Using Agency or the Using Agency's designee to work alongside Contractor Personnel to shadow their role and enable knowledge transfer; answer questions; and explain procedures, tools, utilities, standards and operations used to perform the terminated Services.

9.11. Change Freeze. Unless otherwise approved by the Using Agency or required on an emergency basis to maintain the performance of the Services in accordance with the Performance Standards and SLAs, during the Exit Assistance Period, Contractor will not make or authorize material Changes to: (a) the terminated Services, including to any Equipment, Software or other facilities used to perform the terminated Services; and (b) any contracts entered into by Contractor that relate to the Services (including contracts with Subcontractors).

9.12. Software Licenses. If and as requested by the Using Agency as part of the Exit Assistance Services, Contractor shall: (a) re-assign licenses to the Using Agency or the Using Agency's designee any licenses for which Contractor obtained Required Consents; (b) grant to the Using Agency, effective as of the Termination Date, at no cost to the Using Agency, a license under Contractor's then-current standard license terms made generally available by Contractor to its other commercial customers in and to all Contractor-Provided Software that constitutes generally commercially available Software that was used by Contractor on a dedicated basis to perform the Services and is reasonably required for the continued operation of the supported environment or to enable the Using Agency to receive services substantially similar to the Services for which Contractor utilized such Software; and with respect to such Software, Contractor shall offer to the Using Agency maintenance (including all enhancements and upgrades) at the lesser of a reasonable rate or the rates Contractor offers to other commercial customers for services of a similar nature and scope; (c) grant to the Using Agency, effective as of the Termination Date, a non-exclusive, non-transferable, fully-paid, royalty-free, perpetual, irrevocable, worldwide license following expiration of the Exit Assistance Period in and to all Contractor-Provided Software that does not constitute generally commercially available Software that is incorporated into the supported environment, which license shall extend only to the use of such Software by the Using Agency or its designee (subject to Contractor's reasonable confidentiality requirements) to continue to enable the Using Agency to receive services substantially similar to the Services for which Contractor utilized such Software; and (d) provide the Using Agency with a copy of the Contractor-Provided Software described in this Section in such media as requested by the Using Agency, together with object code and appropriate documentation.

10. Miscellaneous

10.1. Survival. Sections 1 (Definitions for Special Conditions), 4 (Intellectual Property), 7 (Data Security Breach), and 8 (Audit Rights) shall survive the expiration or termination of this Agreement for a period of five (5) years (and Sections 5 (Using Agency Data and Confidentiality) and 10 (Miscellaneous) shall survive for a period of ten [10] years) from the later of (a) the expiration or termination of this Agreement (including any Exit Assistance Period), or (b) the return or destruction of Using Agency Confidential Information as required by this Agreement.

10.2. System Software Updates and Upgrades. Software release level shall not fall more than one (1) level below the most currently published release. All future releases of software should be backward compatible or run concurrently with the previous versions during the update and upgrade process. Updates and upgrades will not require a "forklift" of existing equipment or infrastructure. Installation of updates and upgrades should be pushed out automatically.

10.3. No Waiver of Tort Immunity. Nothing in this Agreement waives immunity available to the Using Agency under Law, including under the Illinois Local Governmental and Governmental Employees Tort Immunity Act, 745 ILCS 10/1-101 et seq.

10.4. No Click-Wrap or Incorporated Terms. The Using Agency is not bound by any content on the Contractor's website, in any click-wrap, shrink-wrap, browse-wrap or other similar document, even if the Contractor's documentation specifically referenced that content and attempts to incorporate it into any other communication, unless the Using Agency has actual knowledge of the content and has expressly agreed to be bound by it in a writing that has been manually signed by the County's Chief Procurement Officer.

10.5. No Limitation. The rights and obligations set forth in these IT special conditions exhibit do not limit the rights and obligations set forth in any Articles of the Professional Services Agreement. For the

avoidance of doubt, the use of County in the PSA or GC shall expressly include Using Agency and vice versa.

10.6. Change Requests. Except as otherwise set forth in this Agreement, this Section 10.5 shall govern all Change Requests and Change Orders. If either Party believes that a Change Order is necessary or desirable, such Party shall submit a Change Request to the other. Contractor represents to Using Agency that it has factored into Contractor's fees adequate contingencies for *de minimis* Change Orders. Accordingly, if Change Requests are made, they will be presumed not to impact the fees under this Agreement; provided, however, that if the Change Request consists of other than a *de minimis* deviation from the scope of the Services and/or Deliverables, Contractor shall provide Using Agency with written notification of such other deviation within five (5) business days after receipt of the Change Request. In the event of a Using Agency-initiated Change Request, within five (5) business days of Contractor's receipt of such Change Request, Contractor shall provide to Using Agency a written statement describing in detail: (a) the reasonably anticipated impact on any Services and Deliverables as a result of the Change Request including, without limitation, Changes in Software and Equipment, and (b) the fixed cost or cost estimate for the Change Request. If Licensor submits a Change Request to Customer, such Change Request shall include the information required for a Change Response.

10.7. Change Orders. Any Change Order that increases the cost or scope of the Agreement, or that materially affects the rights or duties of the Parties as set forth the Agreement, must be agreed upon by the Using Agency in a writing executed by the County's Chief Procurement Officer. In all cases, the approval of all Change Requests and issuance of corresponding Change Orders must comply the County's Procurement Code. If either Party rejects the other's Change Request, Contractor shall proceed to fulfill its obligations under this Agreement.

Appendix XVI – Computer Justice Information Systems [CJIS] Policy



U. S. Department of Justice
Federal Bureau of Investigation
Criminal Justice Information Services Division



Criminal Justice Information Services (CJIS) Security Policy

Version 5.8
06/01/2019

CJISD-ITS-DOC-08140-5.8



Prepared by:
CJIS Information Security Officer

Approved by:
CJIS Advisory Policy Board

EXECUTIVE SUMMARY

Law enforcement needs timely and secure access to services that provide data wherever and whenever for stopping and reducing crime. In response to these needs, the Advisory Policy Board (APB) recommended to the Federal Bureau of Investigation (FBI) that the Criminal Justice Information Services (CJIS) Division authorize the expansion of the existing security management structure in 1998. Administered through a shared management philosophy, the CJIS Security Policy contains information security requirements, guidelines, and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the sources, transmission, storage, and generation of Criminal Justice Information (CJI). The Federal Information Security Management Act of 2002 provides further legal basis for the APB approved management, operational, and technical security requirements mandated to protect CJI and by extension the hardware, software and infrastructure required to enable the services provided by the criminal justice community.

The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

The CJIS Security Policy integrates presidential directives, federal laws, FBI directives and the criminal justice community's APB decisions along with nationally recognized guidance from the National Institute of Standards and Technology. The Policy is presented at both strategic and tactical levels and is periodically updated to reflect the security requirements of evolving business models. The Policy features modular sections enabling more frequent updates to address emerging threats and new security measures. The provided security criteria assists agencies with designing and implementing systems to meet a uniform level of risk and security protection while enabling agencies the latitude to institute more stringent security requirements and controls based on their business model and local needs.

The CJIS Security Policy strengthens the partnership between the FBI and CJIS Systems Agencies (CSA), including, in those states with separate authorities, the State Identification Bureaus (SIB). Further, as use of criminal history record information for noncriminal justice purposes continues to expand, the CJIS Security Policy becomes increasingly important in guiding the National Crime Prevention and Privacy Compact Council and State Compact Officers in the secure exchange of criminal justice records.

The Policy describes the vision and captures the security concepts that set the policies, protections, roles, and responsibilities with minimal impact from changes in technology. The Policy empowers CSAs with the insight and ability to tune their security programs according to their risks, needs, budgets, and resource constraints while remaining compliant with the baseline level of security set forth in this Policy. The CJIS Security Policy provides a secure framework of laws, standards, and elements of published and vetted policies for accomplishing the mission across the broad spectrum of the criminal justice and noncriminal justice communities.

CHANGE MANAGEMENT

Revision	Change Description	Created/Changed by	Date	Approved By
5	Policy Rewrite	Security Policy Working Group	2/9/2011	See Signature Page
5.1	Incorporate Calendar Year 2011 APB approved changes and administrative changes	CJIS ISO Program Office	7/13/2012	APB & Compact Council
5.2	Incorporate Calendar Year 2012 APB approved changes and administrative changes	CJIS ISO Program Office	8/9/2013	APB & Compact Council
5.3	Incorporate Calendar Year 2013 APB approved changes and administrative changes	CJIS ISO Program Office	8/4/2014	APB & Compact Council
5.4	Incorporate Calendar Year 2014 APB approved changes and administrative changes	CJIS ISO Program Office	10/6/2015	APB & Compact Council
5.5	Incorporate Calendar Year 2015 APB approved changes and administrative changes	CJIS ISO Program Office	6/1/2016	APB & Compact Council
5.6	Incorporate Calendar Year 2016 APB approved changes and administrative changes	CJIS ISO Program Office	6/5/2017	APB & Compact Council
5.7	Incorporate Calendar Year 2017 APB approved changes and administrative changes	CJIS ISO Program Office	08/16/2018	APB & Compact Council
5.8	Incorporate Calendar Year 2018 APB approved changes and administrative changes	CJIS ISO Program Office	06/01/2019	APB & Compact Council

SUMMARY OF CHANGES

Version 5.8

APB Approved Changes

1. **Section 3.2.2 CJIS Systems Officer (CSO):** change '2 d.' to read consistent with other bullet appointment requirements, Fall 2018, APB#14, SA#5, Local Agency Security Officers (LASO) Training Requirement.
2. **Section 3.2.2 CJIS Systems Officer (CSO):** add requirement at '2 f.' for LASO training, Fall 2018, APB#14, SA#5, Local Agency Security Officers (LASO) Training Requirement.
3. **Section 4.1 Criminal Justice Information (CJI):** add clarifying language to last paragraph, Fall 2018, APB#14, SA#7, SA Subcommittee Courts Task Force Recommendation.
4. **Section 5.2 Policy Area 2: Security Awareness Training:** add new introductory paragraph, Fall 2018, APB#14, SA#5, Local Agency Security Officers (LASO) Training Requirement.
5. **Section 5.2.1 Awareness Topics:** rename section to "Basic Security Awareness Training", Fall 2018, APB#14, SA#5, Local Agency Security Officers (LASO) Training Requirement.
6. **Section 5.2.2 Security Training Records:** change section title to "LASO Training" and add new requirements, Fall 2018, APB#14, SA#5, Local Agency Security Officers (LASO) Training Requirement.
7. **Section 5.2.3 Security Training Records:** create new section from previous Section 5.2.2, Fall 2018, APB#14, SA#5, Local Agency Security Officers (LASO) Training Requirement.
8. **Section 5.6.2.1.1 Password:** add new introductory paragraph and note, Spring 2018, APB#17, SA#5, Adopting New Standards for Passwords from National Institute of Technologies (NIST) Special Publication 800-63D.
9. **Section 5.6.2.1.1.1 Basic Password Standards:** add new section number and title for existing password requirements, Spring 2018, APB#17, SA#5, Adopting New Standards for Passwords from National Institute of Technologies (NIST) Special Publication 800-63D.
10. **Section 5.6.2.1.1.2 Advanced Password Standards:** add new section and requirements, Spring 2018, APB#17, SA#5, Adopting New Standards for Passwords from National Institute of Technologies (NIST) Special Publication 800-63D.
11. **Section 5.10.1.3 Intrusion Detection Tools and Techniques:** add new introductory paragraph and requirements, Fall 2018, APB#14, SA#3, Intrusion Detection and Prevention Systems.
12. **Section 5.13.2 Mobile Device Management (MDM):** add exception to the MDM requirement for indirect access, Fall 2018, APB#14, SA#2, Mobile Device Management.
13. **Section 5.13.3 Wireless Device Risk Mitigations:** add language to bullets 6 and 7, Fall 2018, APB#14, SA#2, Mobile Device Management.
14. **Section 5.13.7.2 Advanced Authentication:** add language to relax requirement for indirect access, Fall 2018, APB#14, SA#2, Mobile Device Management.
15. **Section 5.13.7.2.1 Compensating Controls:** modify language to clarify requirements, Fall 2018, APB#14, SA#2, Mobile Device Management.

16. **Appendix A Terms and Definitions:** add definitions, “Hashing”, “Hash Value”, “Intrusion Detection”, “Intrusion Detection System”, “Intrusion Prevention”, “Intrusion Prevention System”, “Password Verifier”, “Salting”.
17. **Appendix B Acronyms:** “HIDS”, “HIPS”, “NIDS”, “NIPS”.

Administrative Changes¹

1. Appendix G.7 Incident Response Best Practices, add new appendix
2. Appendix G.8 Secure Coding Best Practices, add new appendix
3. Appendix K, General CJI Guidance, bullet k.: update language based on previous Section 5.12 changes (v5.7).

KEY TO APB APPROVED CHANGES (e.g. “Fall 2013, APB#11, SA#6, Topic Title”):

Fall 2013 – Advisory Policy Board cycle and year

APB## – Advisory Policy Board Topic number

SA## – Security and Access Subcommittee Topic number

Topic Title

¹ Administrative changes are vetted through the Security and Access Subcommittee and not the entire APB process.

TABLE OF CONTENTS

Executive Summary	i
Change Management	ii
Summary of Changes	iii
Table of Contents	v
List of Figures	x
1 Introduction	1
1.1 Purpose	1
1.2 Scope	1
1.3 Relationship to Local Security Policy and Other Policies	1
1.4 Terminology Used in This Document	2
1.5 Distribution of the CJIS Security Policy	2
2 CJIS Security Policy Approach	3
2.1 CJIS Security Policy Vision Statement	3
2.2 Architecture Independent	3
2.3 Risk Versus Realism	3
3 Roles and Responsibilities	4
3.1 Shared Management Philosophy	4
3.2 Roles and Responsibilities for Agencies and Parties	4
3.2.1 CJIS Systems Agencies (CSA)	5
3.2.2 CJIS Systems Officer (CSO)	5
3.2.3 Terminal Agency Coordinator (TAC)	6
3.2.4 Criminal Justice Agency (CJA)	6
3.2.5 Noncriminal Justice Agency (NCJA)	6
3.2.6 Contracting Government Agency (CGA)	7
3.2.7 Agency Coordinator (AC)	7
3.2.8 CJIS Systems Agency Information Security Officer (CSA ISO)	7
3.2.9 Local Agency Security Officer (LASO)	8
3.2.10 FBI CJIS Division Information Security Officer (FBI CJIS ISO)	8
3.2.11 Repository Manager	9
3.2.12 Compact Officer	9
4 Criminal Justice Information and Personally Identifiable Information	10
4.1 Criminal Justice Information (CJI)	10
4.1.1 Criminal History Record Information (CHRI)	10
4.2 Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information	11
4.2.1 Proper Access, Use, and Dissemination of CHRI	11
4.2.2 Proper Access, Use, and Dissemination of NCIC Restricted Files Information	11
4.2.3 Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information	11
4.2.3.1 For Official Purposes	11
4.2.3.2 For Other Authorized Purposes	12
4.2.3.3 CSO Authority in Other Circumstances	12
4.2.4 Storage	12
4.2.5 Justification and Penalties	12

4.2.5.1	Justification	12
4.2.5.2	Penalties	12
4.3	Personally Identifiable Information (PII)	12
5	Policy and Implementation	14
5.1	Policy Area 1: Information Exchange Agreements	15
5.1.1	Information Exchange	15
5.1.1.1	Information Handling	15
5.1.1.2	State and Federal Agency User Agreements	15
5.1.1.3	Criminal Justice Agency User Agreements	16
5.1.1.4	Interagency and Management Control Agreements	16
5.1.1.5	Private Contractor User Agreements and CJIS Security Addendum	16
5.1.1.6	Agency User Agreements	17
5.1.1.7	Outsourcing Standards for Channelers	17
5.1.1.8	Outsourcing Standards for Non-Channelers	18
5.1.2	Monitoring, Review, and Delivery of Services	18
5.1.2.1	Managing Changes to Service Providers	18
5.1.3	Secondary Dissemination	18
5.1.4	Secondary Dissemination of Non-CHRI CJI	18
5.2	Policy Area 2: Security Awareness Training	20
5.2.1	Basic Security Awareness Training	20
5.2.1.1	Level One Security Awareness Training	20
5.2.1.2	Level Two Security Awareness Training	20
5.2.1.3	Level Three Security Awareness Training	21
5.2.1.4	Level Four Security Awareness Training	21
5.2.2	LASO Training	22
5.2.3	Security Training Records	22
5.3	Policy Area 3: Incident Response	24
5.3.1	Reporting Security Events	24
5.3.1.1	Reporting Structure and Responsibilities	24
5.3.1.1.1	FBI CJIS Division Responsibilities	24
5.3.1.1.2	CSA ISO Responsibilities	24
5.3.2	Management of Security Incidents	25
5.3.2.1	Incident Handling	25
5.3.2.2	Collection of Evidence	25
5.3.3	Incident Response Training	25
5.3.4	Incident Monitoring	25
5.4	Policy Area 4: Auditing and Accountability	27
5.4.1	Auditable Events and Content (Information Systems)	27
5.4.1.1	Events	27
5.4.1.1.1	Content	28
5.4.2	Response to Audit Processing Failures	28
5.4.3	Audit Monitoring, Analysis, and Reporting	28
5.4.4	Time Stamps	28
5.4.5	Protection of Audit Information	28
5.4.6	Audit Record Retention	28
5.4.7	Logging NCIC and III Transactions	29

5.5	Policy Area 5: Access Control	30
5.5.1	Account Management	30
5.5.2	Access Enforcement	30
5.5.2.1	Least Privilege	31
5.5.2.2	System Access Control	31
5.5.2.3	Access Control Criteria	31
5.5.2.4	Access Control Mechanisms	31
5.5.3	Unsuccessful Login Attempts	32
5.5.4	System Use Notification	32
5.5.5	Session Lock	32
5.5.6	Remote Access	33
5.5.6.1	Personally Owned Information Systems	33
5.5.6.2	Publicly Accessible Computers	33
5.6	Policy Area 6: Identification and Authentication	35
5.6.1	Identification Policy and Procedures	35
5.6.1.1	Use of Originating Agency Identifiers in Transactions and Information Exchanges	35
5.6.2	Authentication Policy and Procedures	35
5.6.2.1	Standard Authenticators	36
5.6.2.1.1	Password	36
5.6.2.1.2	Personal Identification Number (PIN)	38
5.6.2.1.3	One-time Passwords (OTP)	38
5.6.2.2	Advanced Authentication	38
5.6.2.2.1	Advanced Authentication Policy and Rationale	39
5.6.2.2.2	Advanced Authentication Decision Tree	39
5.6.3	Identifier and Authenticator Management	41
5.6.3.1	Identifier Management	41
5.6.3.2	Authenticator Management	42
5.6.4	Assertions	42
5.7	Policy Area 7: Configuration Management	48
5.7.1	Access Restrictions for Changes	48
5.7.1.1	Least Functionality	48
5.7.1.2	Network Diagram	48
5.7.2	Security of Configuration Documentation	48
5.8	Policy Area 8: Media Protection	49
5.8.1	Media Storage and Access	49
5.8.2	Media Transport	49
5.8.2.1	Digital Media during Transport	49
5.8.2.2	Physical Media in Transit	49
5.8.3	Digital Media Sanitization and Disposal	49
5.8.4	Disposal of Physical Media	49
5.9	Policy Area 9: Physical Protection	51
5.9.1	Physically Secure Location	51
5.9.1.1	Security Perimeter	51
5.9.1.2	Physical Access Authorizations	51
5.9.1.3	Physical Access Control	51

5.9.1.4	Access Control for Transmission Medium	51
5.9.1.5	Access Control for Display Medium	51
5.9.1.6	Monitoring Physical Access	52
5.9.1.7	Visitor Control	52
5.9.1.8	Delivery and Removal	52
5.9.2	Controlled Area	52
5.10	Policy Area 10: System and Communications Protection and Information Integrity	53
5.10.1	Information Flow Enforcement	53
5.10.1.1	Boundary Protection	53
5.10.1.2	Encryption	54
5.10.1.2.1	Encryption for CJI in Transit	54
5.10.1.2.2	Encryption for CJI at Rest	55
5.10.1.2.3	Public Key Infrastructure (PKI) Technology	55
5.10.1.3	Intrusion Detection Tools and Techniques	55
5.10.1.4	Voice over Internet Protocol	56
5.10.1.5	Cloud Computing	56
5.10.2	Facsimile Transmission of CJI	57
5.10.3	Partitioning and Virtualization	57
5.10.3.1	Partitioning	57
5.10.3.2	Virtualization	58
5.10.4	System and Information Integrity Policy and Procedures	58
5.10.4.1	Patch Management	58
5.10.4.2	Malicious Code Protection	59
5.10.4.3	Spam and Spyware Protection	59
5.10.4.4	Security Alerts and Advisories	59
5.10.4.5	Information Input Restrictions	60
5.11	Policy Area 11: Formal Audits	61
5.11.1	Audits by the FBI CJIS Division	61
5.11.1.1	Triennial Compliance Audits by the FBI CJIS Division	61
5.11.1.2	Triennial Security Audits by the FBI CJIS Division	61
5.11.2	Audits by the CSA	61
5.11.3	Special Security Inquiries and Audits	62
5.11.4	Compliance Subcommittees	62
5.12	Policy Area 12: Personnel Security	63
5.12.1	Personnel Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJI	63
5.12.2	Personnel Termination	64
5.12.3	Personnel Transfer	64
5.12.4	Personnel Sanctions	64
5.13	Policy Area 13: Mobile Devices	66
5.13.1	Wireless Communications Technologies	66
5.13.1.1	802.11 Wireless Protocols	66
5.13.1.2	Cellular Devices	67
5.13.1.2.1	Cellular Service Abroad	68
5.13.1.2.2	Voice Transmissions Over Cellular Devices	68
5.13.1.3	Bluetooth	68

5.13.1.4 Mobile Hotspots.....	68
5.13.2 Mobile Device Management (MDM)	69
5.13.3 Wireless Device Risk Mitigations	69
5.13.4 System Integrity	70
5.13.4.1 Patching/Updates	70
5.13.4.2 Malicious Code Protection.....	70
5.13.4.3 Personal Firewall	70
5.13.5 Incident Response	71
5.13.6 Access Control	71
5.13.7 Identification and Authentication.....	71
5.13.7.1 Local Device Authentication	71
5.13.7.2 Advanced Authentication.....	72
5.13.7.2.1 Compensating Controls.....	72
5.13.7.3 Device Certificates.....	72
Appendices.....	A-1
Appendix A Terms and Definitions	A-1
Appendix B Acronyms.....	B-1
Appendix C Network Topology Diagrams	C-1
Appendix D Sample Information Exchange Agreements.....	D-1
D.1 CJIS User Agreement	D-1
D.2 Management Control Agreement.....	D-9
D.3 Noncriminal Justice Agency Agreement & Memorandum of Understanding.....	D-10
D.4 Interagency Connection Agreement	D-16
Appendix E Security Forums and Organizational Entities.....	E-1
Appendix F Sample Forms.....	F-1
F.1 Security Incident Response Form	F-2
Appendix G Best practices.....	G-1
G.1 Virtualization	G-1
G.2 Voice over Internet Protocol	G-4
G.3 Cloud Computing.....	G-15
G.4 Mobile Appendix	G-32
G.5 Administrator Accounts for Least Privilege and Separation of Duties.....	G-53
G.6 Encryption.....	G-66
G.7 Incident Response	G-1
G.8 Secure Coding.....	G-1
Appendix H Security Addendum	H-1
Appendix I References.....	I-1
Appendix J Noncriminal Justice Agency Supplemental Guidance	J-1
Appendix K Criminal Justice Agency Supplemental Guidance	K-1

LIST OF FIGURES

Figure 1 – Overview Diagram of Strategic Functions and Policy Components.....	4
Figure 2 – Dissemination of restricted and non-restricted NCIC data.....	13
Figure 3 – Information Exchange Agreements Implemented by a Local Police Department	19
Figure 4 – Security Awareness Training Use Cases.....	22
Figure 5 – Incident Response Process Initiated by an Incident in a Local Police Department	26
Figure 6 – Local Police Department's Use of Audit Logs	29
Figure 7 – A Local Police Department's Access Controls	34
Figure 8 – Advanced Authentication Use Cases.....	42
Figure 9 – Authentication Decision for Known Location	46
Figure 10 – Authentication Decision for Unknown Location	47
Figure 11 – A Local Police Department's Configuration Management Controls	48
Figure 12 – A Local Police Department's Media Management Policies	50
Figure 13 – A Local Police Department's Physical Protection Measures.....	52
Figure 14 – System and Communications Protection and Information Integrity Use Cases.....	60
Figure 15 – The Audit of a Local Police Department.....	62
Figure 16 – A Local Police Department's Personnel Security Controls	64

1 INTRODUCTION

This section details the purpose of this document, its scope, relationship to other information security policies, and its distribution constraints.

1.1 Purpose

The CJIS Security Policy provides Criminal Justice Agencies (CJA) and Noncriminal Justice Agencies (NCJA) with a minimum set of security requirements for access to Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division systems and information and to protect and safeguard Criminal Justice Information (CJI). This minimum standard of security requirements ensures continuity of information protection. The essential premise of the CJIS Security Policy is to provide the appropriate controls to protect CJI, from creation through dissemination; whether at rest or in transit.

The CJIS Security Policy integrates presidential directives, federal laws, FBI directives, the criminal justice community's Advisory Policy Board (APB) decisions along with nationally recognized guidance from the National Institute of Standards and Technology (NIST) and the National Crime Prevention and Privacy Compact Council (Compact Council).

1.2 Scope

At the consent of the advisory process, and taking into consideration federal law and state statutes, the CJIS Security Policy applies to all entities with access to, or who operate in support of, FBI CJIS Division's services and information. The CJIS Security Policy provides minimum security requirements associated with the creation, viewing, modification, transmission, dissemination, storage, or destruction of CJI.

Entities engaged in the interstate exchange of CJI data for noncriminal justice purposes are also governed by the standards and rules promulgated by the Compact Council.

1.3 Relationship to Local Security Policy and Other Policies

The CJIS Security Policy may be used as the sole security policy for the agency. The local agency may complement the CJIS Security Policy with a local policy, or the agency may develop their own stand-alone security policy; however, the CJIS Security Policy shall always be the minimum standard and local policy may augment, or increase the standards, but shall not detract from the CJIS Security Policy standards.

The agency shall develop, disseminate, and maintain formal, documented procedures to facilitate the implementation of the CJIS Security Policy and, where applicable, the local security policy. The policies and procedures shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. Procedures developed for CJIS Security Policy areas can be developed for the security program in general, and for a particular information system, when required.

This document is a compendium of applicable policies in providing guidance on the minimum security controls and requirements needed to access FBI CJIS information and services. These policies include presidential directives, federal laws, FBI directives and the criminal justice community's APB decisions. State, local, and Tribal CJA may implement more stringent policies

and requirements. Appendix I contains the references while Appendix E lists the security forums and organizational entities referenced in this document.

1.4 Terminology Used in This Document

The following terms are used interchangeably throughout this document:

- **Agency and Organization:** The two terms in this document refer to any entity that submits or receives information, by any means, to/from FBI CJIS systems or services.
- **Information and Data:** Both terms refer to CJI.
- **System, Information System, Service, or named applications like NCIC:** all refer to connections to the FBI's criminal justice information repositories and the equipment used to establish said connections.
- **References/Citations/Directives:** Appendix I contains all of the references used in this Policy and may contain additional sources that could apply to any section.

Appendix A and B provide an extensive list of the terms and acronyms.

1.5 Distribution of the CJIS Security Policy

The CJIS Security Policy, version 5.0 and later, is a publicly available document and may be posted and shared without restrictions.

2 CJIS SECURITY POLICY APPROACH

The CJIS Security Policy represents the shared responsibility between FBI CJIS, CJIS Systems Agency (CSA), and the State Identification Bureaus (SIB) of the lawful use and appropriate protection of CJL. The Policy provides a baseline of security requirements for current and planned services and sets a minimum standard for new initiatives.

2.1 CJIS Security Policy Vision Statement

The executive summary of this document describes the vision in terms of business needs for confidentiality, integrity, and availability of information. The APB collaborates with the FBI CJIS Division to ensure that the Policy remains updated to meet evolving business, technology and security needs.

2.2 Architecture Independent

Due to advancing technology and evolving business models, the FBI CJIS Division is transitioning from legacy stovepipe systems and moving toward a flexible services approach. Systems such as National Crime Information Center (NCIC), National Instant Criminal Background Check System (NICS), and Next Generation Identification (NGI) will continue to evolve and may no longer retain their current system platforms, hardware, or program name. However, the data and services provided by these systems will remain stable.

The CJIS Security Policy looks at the data (information), services, and protection controls that apply regardless of the implementation architecture. Architectural independence is not intended to lessen the importance of systems, but provide for the replacement of one technology with another while ensuring the controls required to protect the information remain constant. This objective and conceptual focus on security policy areas provide the guidance and standards while avoiding the impact of the constantly changing landscape of technical innovations. The architectural independence of the Policy provides agencies with the flexibility for tuning their information security infrastructure and policies to reflect their own environments.

2.3 Risk Versus Realism

Every “shall” statement contained within the CJIS Security Policy has been scrutinized for risk versus the reality of resource constraints and real-world application. The purpose of the CJIS Security Policy is to establish the minimum security requirements; therefore, individual agencies are encouraged to implement additional controls to address agency specific risks. Each agency faces risk unique to that agency. It is quite possible that several agencies could encounter the same type of risk however depending on resources would mitigate that risk differently. In that light, a risk-based approach can be used when implementing requirements.

3 ROLES AND RESPONSIBILITIES

3.1 Shared Management Philosophy

In the scope of information security, the FBI CJIS Division employs a shared management philosophy with federal, state, local, and tribal law enforcement agencies. Although an advisory policy board for the NCIC has existed since 1969, the Director of the FBI established the CJIS APB in March 1994 to enable appropriate input and recommend policy with respect to CJIS services. Through the APB and its Subcommittees and Working Groups, consideration is given to the needs of the criminal justice and law enforcement community regarding public policy, statutory and privacy aspects, as well as national security relative to CJIS systems and information. The APB represents federal, state, local, and tribal law enforcement and criminal justice agencies throughout the United States, its territories, and Canada.

The FBI has a similar relationship with the Compact Council, which governs the interstate exchange of criminal history records for noncriminal justice purposes. The Compact Council is mandated by federal law to promulgate rules and procedures for the use of the Interstate Identification Index (III) for noncriminal justice purposes. To meet that responsibility, the Compact Council depends on the CJIS Security Policy as the definitive source for standards defining the security and privacy of records exchanged with noncriminal justice practitioners.

3.2 Roles and Responsibilities for Agencies and Parties

It is the responsibility of all agencies covered under this Policy to ensure the protection of CJI between the FBI CJIS Division and its user community. The following figure provides an abstract representation of the strategic functions and roles such as governance and operations.

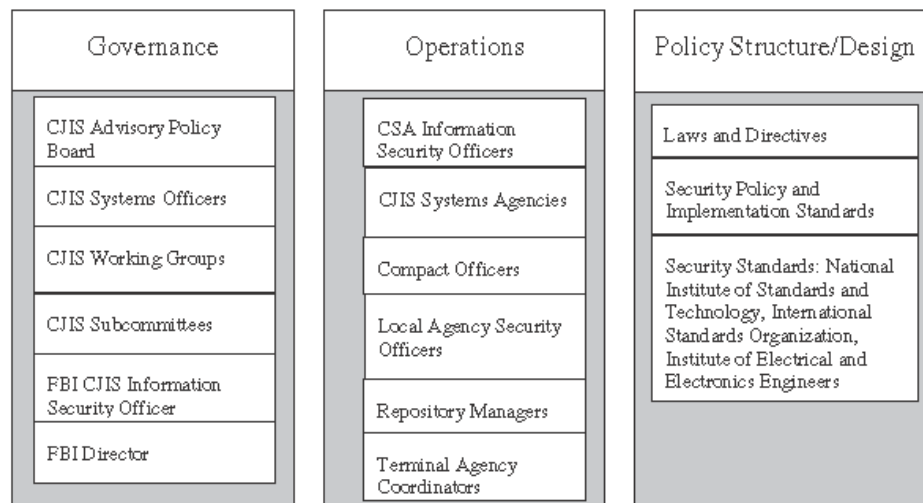


Figure 1 – Overview Diagram of Strategic Functions and Policy Components

This section provides a description of the following entities and roles:

1. CJIS Systems Agency.
2. CJIS Systems Officer.
3. Terminal Agency Coordinator.
4. Criminal Justice Agency.
5. Noncriminal Justice Agency.
6. Contracting Government Agency.
7. Agency Coordinator.
8. CJIS Systems Agency Information Security Officer.
9. Local Agency Security Officer.
10. FBI CJIS Division Information Security Officer.
11. Repository Manager.
12. Compact Officer.

3.2.1 CJIS Systems Agencies (CSA)

The CSA is responsible for establishing and administering an information technology security program throughout the CSA's user community, to include the local levels. The head of each CSA shall appoint a CJIS Systems Officer (CSO). The CSA may impose more stringent protection measures than outlined in this document. Such decisions shall be documented and kept current.

3.2.2 CJIS Systems Officer (CSO)

The CSO is an individual located within the CSA responsible for the administration of the CJIS network for the CSA. Pursuant to the Bylaws for the CJIS Advisory Policy Board and Working Groups, the role of CSO shall not be outsourced. The CSO may delegate responsibilities to subordinate agencies. The CSO shall set, maintain, and enforce the following:

1. Standards for the selection, supervision, and separation of personnel who have access to CJIS.
2. Policy governing the operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that comprise and support a telecommunications network and related CJIS systems used to process, store, or transmit CJIS, guaranteeing the priority, confidentiality, integrity, and availability of service needed by the criminal justice community.
 - a. Ensure appropriate use, enforce system discipline, and ensure CJIS Division operating procedures are followed by all users of the respective services and information.
 - b. Ensure state/federal agency compliance with policies approved by the APB and adopted by the FBI.

- c. Ensure the appointment of the CSA ISO and determine the extent of authority to the CSA ISO.
 - d. Ensure the designation of a Terminal Agency Coordinator (TAC) within each agency with devices accessing CJIS systems.
 - e. Ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO).
 - f. Ensure each LASO receives enhanced security awareness training (ref. Section 5.2).
 - g. Approve access to FBI CJIS systems.
 - h. Assume ultimate responsibility for managing the security of CJIS systems within their state and/or agency.
 - i. Perform other related duties outlined by the user agreements with the FBI CJIS Division.
3. Outsourcing of Criminal Justice Functions
- a. Responsibility for the management of the approved security requirements shall remain with the CJA. Security control includes the authority to enforce the standards for the selection, supervision, and separation of personnel who have access to CJI; set and enforce policy governing the operation of computers, circuits, and telecommunications terminals used to process, store, or transmit CJI; and to guarantee the priority service needed by the criminal justice community.
 - b. Responsibility for the management control of network security shall remain with the CJA. Management control of network security includes the authority to enforce the standards for the selection, supervision, and separation of personnel who have access to CJI; set and enforce policy governing the operation of circuits and network equipment used to transmit CJI; and to guarantee the priority service as determined by the criminal justice community.

3.2.3 Terminal Agency Coordinator (TAC)

The TAC serves as the point-of-contact at the local agency for matters relating to CJIS information access. The TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with CJIS systems policies.

3.2.4 Criminal Justice Agency (CJA)

A CJA is defined as a court, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

3.2.5 Noncriminal Justice Agency (NCJA)

A NCJA is defined (for the purposes of access to CJI) as an entity or any subunit thereof that provides services primarily for purposes other than the administration of criminal justice.

3.2.6 Contracting Government Agency (CGA)

A CGA is a government agency, whether a CJA or a NCJA, that enters into an agreement with a private contractor subject to the CJIS Security Addendum. The CGA entering into an agreement with a contractor shall appoint an agency coordinator.

3.2.7 Agency Coordinator (AC)

An AC is a staff member of the CGA who manages the agreement between the Contractor and agency. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC. The AC shall:

1. Understand the communications, records capabilities, and needs of the Contractor which is accessing federal and state records through or because of its relationship with the CGA.
2. Participate in related meetings and provide input and comments for system improvement.
3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.
4. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor.
5. Maintain up-to-date records of Contractor's employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable).
6. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with permission from the CSA staff. Schedule new operators for the certification exam within six (6) months of assignment. Schedule certified operators for biennial recertification testing within thirty (30) days prior to the expiration of certification. Schedule operators for other mandated class.
7. The AC will not permit an untrained/untested or non-certified Contractor employee to access CJI or systems supporting CJI where access to CJI can be gained.
8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.
9. Provide completed applicant fingerprint cards on each Contractor employee who accesses the system to the CGA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system.
10. Any other responsibility for the AC promulgated by the FBI.

3.2.8 CJIS Systems Agency Information Security Officer (CSA ISO)

The CSA ISO shall:

1. Serve as the security point of contact (POC) to the FBI CJIS Division ISO.

2. Document technical compliance with the CJIS Security Policy with the goal to assure the confidentiality, integrity, and availability of criminal justice information to the user community throughout the CSA's user community, to include the local level.
3. Document and provide assistance for implementing the security-related controls for the Interface Agency and its users.
4. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.

3.2.9 Local Agency Security Officer (LASO)

Each LASO shall:

1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in this Policy.
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

3.2.10 FBI CJIS Division Information Security Officer (FBI CJIS ISO)

The FBI CJIS ISO shall:

1. Maintain the CJIS Security Policy.
2. Disseminate the FBI Director approved CJIS Security Policy.
3. Serve as a liaison with the CSA's ISO and with other personnel across the CJIS community and in this regard provide technical guidance as to the intent and implementation of operational and technical policy issues.
4. Serve as a point-of-contact (POC) for computer incident notification and distribution of security alerts to the CSOs and ISOs.
5. Assist with developing audit compliance guidelines as well as identifying and reconciling security-related issues.
6. Develop and participate in information security training programs for the CSOs and ISOs, and provide a means by which to acquire feedback to measure the effectiveness and success of such training.
7. Maintain a security policy resource center (SPRC) on FBI.gov and keep the CSOs and ISOs updated on pertinent information.

3.2.11 Repository Manager

The State Identification Bureau (SIB) Chief, i.e. Repository Manager or Chief Administrator, is the designated manager of the agency having oversight responsibility for a state's fingerprint identification services. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the SIB Chief and CSO may be the same person.

3.2.12 Compact Officer

Pursuant to the National Crime Prevention and Privacy Compact, each party state shall appoint a Compact Officer who shall ensure that Compact provisions and rules, procedures, and standards established by the Compact Council are complied with in their respective state.

4 CRIMINAL JUSTICE INFORMATION AND PERSONALLY IDENTIFIABLE INFORMATION

4.1 Criminal Justice Information (CJI)

Criminal Justice Information is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:

1. Biometric Data—data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data.
2. Identity History Data—textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual.
3. Biographic Data—information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.
4. Property Data—information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII).
5. Case/Incident History—information about the history of criminal incidents.

The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g., ORI, NIC, UCN, etc.) when not accompanied by information that reveals CJI or PII.

The intent of the CJIS Security Policy is to ensure the protection of the aforementioned CJI until the information is: released to the public via authorized dissemination (e.g. within a court system; presented in crime reports data; released in the interest of public safety); purged or destroyed in accordance with applicable record retention rules. CJI introduced into the court system pursuant to a judicial proceeding and that can be released to the public via a public records request is not subject to the CJIS Security Policy.

4.1.1 Criminal History Record Information (CHRI)

Criminal History Record Information (CHRI), sometimes informally referred to as “restricted data”, is a subset of CJI. Due to its comparatively sensitive nature, additional controls are required for the access, use and dissemination of CHRI. In addition to the dissemination restrictions outlined below, Title 28, Part 20, Code of Federal Regulations (CFR), defines CHRI and provides the regulatory guidance for dissemination of CHRI. While the CJIS Security Policy attempts to be architecturally independent, the III and the NCIC are specifically identified in Title 28, Part 20, CFR, and the NCIC Operating Manual, as associated with CHRI.

4.2 Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information

This section describes the requirements for the access, use and dissemination of CHRI, NCIC restricted files information, and NCIC non-restricted files information.

4.2.1 Proper Access, Use, and Dissemination of CHRI

Information obtained from the III is considered CHRI. Rules governing the access, use, and dissemination of CHRI are found in Title 28, Part 20, CFR. The III shall be accessed only for an authorized purpose. Further, CHRI shall only be used for an authorized purpose consistent with the purpose for which III was accessed. Dissemination to another agency is authorized if (a) the other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or (b) the other agency is performing personnel and appointment functions for criminal justice employment applicants.

4.2.2 Proper Access, Use, and Dissemination of NCIC Restricted Files Information

The NCIC hosts restricted files and non-restricted files. NCIC restricted files are distinguished from NCIC non-restricted files by the policies governing their access and use. Proper access to, use, and dissemination of data from restricted files shall be consistent with the access, use, and dissemination policies concerning the III described in Title 28, Part 20, CFR, and the NCIC Operating Manual. The restricted files, which shall be protected as CHRI, are as follows:

1. Gang Files
2. Known or Appropriately Suspected Terrorist Files
3. Supervised Release Files
4. National Sex Offender Registry Files
5. Historical Protection Order Files of the NCIC
6. Identity Theft Files
7. Protective Interest Files
8. Person With Information (PWI) data in the Missing Person Files
9. Violent Person File
10. NICS Denied Transactions File

The remaining NCIC files are considered non-restricted files.

4.2.3 Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information

4.2.3.1 For Official Purposes

NCIC non-restricted files are those not listed as restricted files in Section 4.2.2. NCIC non-restricted files information may be accessed and used for any authorized purpose consistent with

the inquiring agency's responsibility. Information obtained may be disseminated to (a) other government agencies or (b) private entities authorized by law to receive such information for any purpose consistent with their responsibilities.

4.2.3.2 For Other Authorized Purposes

NCIC non-restricted files may be accessed for other purposes consistent with the resources of the inquiring agency; however, requests for bulk data are discouraged. Information derived from NCIC non-restricted files for other than law enforcement purposes can be used by authorized criminal justice personnel only to confirm the status of a person or property (i.e., wanted or stolen). An inquiring agency is authorized to charge a nominal administrative fee for such service. Non-restricted files information shall not be disseminated commercially.

A response to a NCIC person inquiry may include NCIC restricted files information as well as NCIC non-restricted files information. Agencies shall not disseminate restricted files information for purposes other than law enforcement.

4.2.3.3 CSO Authority in Other Circumstances

If no federal, state or local law or policy prohibition exists, the CSO may exercise discretion to approve or deny dissemination of NCIC non-restricted file information.

4.2.4 Storage

When CHRI is stored, agencies shall establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of the information. These records shall be stored for extended periods only when they are key elements for the integrity and/or utility of case files and/or criminal record files. See Section 5.9 for physical security controls.

4.2.5 Justification and Penalties

4.2.5.1 Justification

In addition to the use of purpose codes and logging information, all users shall provide a reason for all III inquiries whenever requested by NCIC System Managers, CSAs, local agency administrators, or their representatives.

4.2.5.2 Penalties

Improper access, use or dissemination of CHRI and NCIC Non-Restricted Files information is serious and may result in administrative sanctions including, but not limited to, termination of services and state and federal criminal penalties.

4.3 Personally Identifiable Information (PII)

For the purposes of this document, PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. Any FBI CJIS provided data maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history may include PII. A criminal history record for

example inherently contains PII as would a Law Enforcement National Data Exchange (N-DEx) case file.

PII shall be extracted from CJI for the purpose of official business only. Agencies shall develop policies, based on state and local privacy rules, to ensure appropriate controls are applied when handling PII extracted from CJI. Due to the expansive nature of PII, this Policy does not specify auditing, logging, or personnel security requirements associated with the life cycle of PII.

Figure 2 – Dissemination of restricted and non-restricted NCIC data

A citizen of Springfield went to the Springfield Police Department to request whether his new neighbor, who had been acting suspiciously, had an outstanding warrant. The Springfield Police Department ran an NCIC persons inquiry, which produced a response that included a Wanted Person File (non-restricted file) record and a Known or Appropriately Suspected Terrorist File (restricted file) record. The Springfield Police Department advised the citizen of the outstanding warrant, but did not disclose any information concerning the subject being a known or appropriately suspected terrorist.

5 POLICY AND IMPLEMENTATION

The policy areas focus upon the data and services that the FBI CJIS Division exchanges and provides to the criminal justice community and its partners. Each policy area provides both strategic reasoning and tactical implementation requirements and standards.

While the major theme of the policy areas is concerned with electronic exchange directly with the FBI, it is understood that further dissemination of CJI to Authorized Recipients by various means (hard copy, e-mail, web posting, etc.) constitutes a significant portion of CJI exchanges. Regardless of its form, use, or method of dissemination, CJI requires protection throughout its life.

Not every consumer of FBI CJIS services will encounter all of the policy areas therefore the circumstances of applicability are based on individual agency/entity configurations and usage. Use cases within each of the policy areas will help users relate the Policy to their own agency circumstances. The policy areas are:

- Policy Area 1—Information Exchange Agreements
- Policy Area 2—Security Awareness Training
- Policy Area 3—Incident Response
- Policy Area 4—Auditing and Accountability
- Policy Area 5—Access Control
- Policy Area 6—Identification and Authentication
- Policy Area 7—Configuration Management
- Policy Area 8—Media Protection
- Policy Area 9—Physical Protection
- Policy Area 10—Systems and Communications Protection and Information Integrity
- Policy Area 11—Formal Audits
- Policy Area 12—Personnel Security
- Policy Area 13—Mobile Devices

5.1 Policy Area 1: Information Exchange Agreements

The information shared through communication mediums shall be protected with appropriate security safeguards. The agreements established by entities sharing information across systems and communications mediums are vital to ensuring all parties fully understand and agree to a set of security standards.

5.1.1 Information Exchange

Before exchanging CJI, agencies shall put formal agreements in place that specify security controls. The exchange of information may take several forms including electronic mail, instant messages, web services, facsimile, hard copy, and information systems sending, receiving and storing CJI.

Information exchange agreements outline the roles, responsibilities, and data ownership between agencies and any external parties. Information exchange agreements for agencies sharing CJI data that is sent to and/or received from the FBI CJIS shall specify the security controls and conditions described in this document.

Information exchange agreements shall be supported by documentation committing both parties to the terms of information exchange. As described in subsequent sections, different agreements and policies apply, depending on whether the parties involved are CJAs or NCJAs. See Appendix D for examples of Information Exchange Agreements.

There may be instances, on an ad-hoc basis, where CJI is authorized for further dissemination to Authorized Recipients not covered by an information exchange agreement with the releasing agency. In these instances the dissemination of CJI is considered to be secondary dissemination. Law Enforcement and civil agencies shall have a local policy to validate a requestor of CJI as an authorized recipient before disseminating CJI. See Section 5.1.3 for secondary dissemination guidance.

5.1.1.1 Information Handling

Procedures for handling and storage of information shall be established to protect that information from unauthorized disclosure, alteration or misuse. Using the requirements in this Policy as a starting point, the procedures shall apply to the handling, processing, storing, and communication of CJI. These procedures apply to the exchange of CJI no matter the form of exchange.

The policies for information handling and protection also apply to using CJI shared with or received from FBI CJIS for noncriminal justice purposes. In general, a noncriminal justice purpose includes the use of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including – but not limited to – employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

5.1.1.2 State and Federal Agency User Agreements

Each CSA head or SIB Chief shall execute a signed written user agreement with the FBI CJIS Division stating their willingness to demonstrate conformity with this Policy before accessing and participating in CJIS records information programs. This agreement shall include the standards and sanctions governing utilization of CJIS systems. As coordinated through the particular CSA

or SIB Chief, each Interface Agency shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system. All user agreements with the FBI CJIS Division shall be coordinated with the CSA head.

5.1.1.3 Criminal Justice Agency User Agreements

Any CJA receiving access to CJIS shall enter into a signed written agreement with the appropriate signatory authority of the CSA providing the access. The written agreement shall specify the FBI CJIS systems and services to which the agency will have access, and the FBI CJIS Division policies to which the agency must adhere. These agreements shall include:

1. Audit.
2. Dissemination.
3. Hit confirmation.
4. Logging.
5. Quality Assurance (QA).
6. Screening (Pre-Employment).
7. Security.
8. Timeliness.
9. Training.
10. Use of the system.
11. Validation.

5.1.1.4 Interagency and Management Control Agreements

A NCJA (government) designated to perform criminal justice functions for a CJA shall be eligible for access to the CJIS. Access shall be permitted when such designation is authorized pursuant to executive order, statute, regulation, or interagency agreement. The NCJA shall sign and execute a management control agreement (MCA) with the CJA, which stipulates management control of the criminal justice function remains solely with the CJA. The MCA may be a separate document or included with the language of an interagency agreement. An example of an NCJA (government) is a city information technology (IT) department.

5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum

The CJIS Security Addendum is a uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to CHRI, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information is consistent with existing regulations and the CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require.

Private contractors who perform criminal justice functions shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies. All private contractors who perform criminal justice functions shall acknowledge, via signing of the CJIS Security

Addendum Certification page, and abide by all aspects of the CJIS Security Addendum. The CJIS Security Addendum is presented in Appendix H. Modifications to the CJIS Security Addendum shall be enacted only by the FBI.

1. Private contractors designated to perform criminal justice functions for a CJA shall be eligible for access to CJI. Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement between the CJA and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).
2. Private contractors designated to perform criminal justice functions on behalf of a NCJA (government) shall be eligible for access to CJI. Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement between the NCJA and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).

5.1.1.6 Agency User Agreements

A NCJA (public) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. A NCJA (public) receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA/SIB providing the access. An example of a NCJA (public) is a county school board.

A NCJA (private) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. A NCJA (private) receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA, SIB, or authorized agency providing the access. An example of a NCJA (private) is a local bank.

All NCJAs accessing CJI shall be subject to all pertinent areas of the CJIS Security Policy (see Appendix J for supplemental guidance). Each NCJA that directly accesses FBI CJI shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system.

5.1.1.7 Outsourcing Standards for Channelers

Channelers designated to request civil fingerprint-based background checks or noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All Channelers accessing CJI shall be subject to the terms and conditions described in the Compact

Council Security and Management Control Outsourcing Standard. Each Channeler that directly accesses CJI shall also allow the FBI to conduct periodic penetration testing.

Channelers leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.

5.1.1.8 Outsourcing Standards for Non-Channelers

Contractors designated to perform noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All contractors accessing CJI shall be subject to the terms and conditions described in the Compact Council Outsourcing Standard for Non-Channelers. Contractors leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.

5.1.2 Monitoring, Review, and Delivery of Services

As specified in the interagency agreements, MCAs, and contractual agreements with private contractors, the services, reports and records provided by the service provider shall be regularly monitored and reviewed. The CJA, authorized agency, or FBI shall maintain sufficient overall control and visibility into all security aspects to include, but not limited to, identification of vulnerabilities and information security incident reporting/response. The incident reporting/response process used by the service provider shall conform to the incident reporting/response specifications provided in this Policy.

5.1.2.1 Managing Changes to Service Providers

Any changes to services provided by a service provider shall be managed by the CJA, authorized agency, or FBI. This includes provision of services, changes to existing services, and new services. Evaluation of the risks to the agency shall be undertaken based on the criticality of the data, system, and the impact of the change.

5.1.3 Secondary Dissemination

If CHRI is released to another authorized agency, and that agency was not part of the releasing agency's primary information exchange agreement(s), the releasing agency shall log such dissemination.

5.1.4 Secondary Dissemination of Non-CHRI CJI

If CJI does not contain CHRI and is not part of an information exchange agreement then it does not need to be logged. Dissemination shall conform to the local policy validating the requestor of the CJI as an employee and/or contractor of a law enforcement agency or civil agency requiring the CJI to perform their mission or a member of the public receiving CJI via authorized dissemination.

Figure 3 – Information Exchange Agreements Implemented by a Local Police Department

A local police department executed a Memorandum of Understanding (MOU) for the interface with their state CSA. The local police department also executed an MOU (which included an MCA) with the county information technology (IT) department for the day-to-day operations of their criminal-justice infrastructure. The county IT department, in turn, outsourced operations to a local vendor who signed the CJIS Security Addendum.

5.2 Policy Area 2: Security Awareness Training

Security training is key to the human element of information security. All users with authorized access to CJI should be made aware of their individual responsibilities and expected behavior when accessing CJI and the systems which process CJI. LASOs require enhanced training on the specific duties and responsibilities of those positions and the impact those positions have on the overall security of information systems.

5.2.1 Basic Security Awareness Training

Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI to include all personnel who have unescorted access to a physically secure location. The CSO/SIB Chief may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.

A significant number of topics can be mentioned and briefly discussed in any awareness session or campaign. To help further the development and implementation of individual agency security awareness training programs the following baseline guidance is provided.

5.2.1.1 Level One Security Awareness Training

At a minimum, the following topics shall be addressed as baseline security awareness training for all personnel who have unescorted access to a physically secure location:

1. Individual responsibilities and expected behavior with regard to being in the vicinity of CJI usage and/or terminals.
2. Implications of noncompliance.
3. Incident response (Identify points of contact and individual actions).
4. Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity, etc.

5.2.1.2 Level Two Security Awareness Training

In addition to 5.2.1.1 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with access to CJI:

1. Media protection.
2. Protect information subject to confidentiality concerns — hardcopy through destruction.
3. Proper handling and marking of CJI.
4. Threats, vulnerabilities, and risks associated with handling of CJI.
5. Social engineering.
6. Dissemination and destruction.

5.2.1.3 Level Three Security Awareness Training

In addition to 5.2.1.1 and 5.2.1.2 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with both physical and logical access to CJI:

1. Rules that describe responsibilities and expected behavior with regard to information system usage.
2. Password usage and management—including creation, frequency of changes, and protection.
3. Protection from viruses, worms, Trojan horses, and other malicious code.
4. Unknown e-mail/attachments.
5. Web usage—allowed versus prohibited; monitoring of user activity.
6. Spam.
7. Physical Security—increases in risks to systems and data.
8. Handheld device security issues—address both physical and wireless security issues.
9. Use of encryption and the transmission of sensitive/confidential information over the Internet—address agency policy, procedures, and technical contact for assistance.
10. Laptop security—address both physical and information security issues.
11. Personally owned equipment and software—state whether allowed or not (e.g., copyrights).
12. Access control issues—address least privilege and separation of duties.
13. Individual accountability—explain what this means in the agency.
14. Use of acknowledgement statements—passwords, access to systems and data, personal use and gain.
15. Desktop security—discuss use of screensavers, restricting visitors' view of information on screen (mitigating "shoulder surfing"), battery backup devices, allowed access to systems.
16. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed.
17. Threats, vulnerabilities, and risks associated with accessing CJIS Service systems and services.

5.2.1.4 Level Four Security Awareness Training

In addition to 5.2.1.1, 5.2.1.2, and 5.1.2.3 above, the following topics at a minimum shall be addressed as baseline security awareness training for all Information Technology personnel (system administrators, security administrators, network administrators, etc.):

1. Protection from viruses, worms, Trojan horses, and other malicious code—scanning, updating definitions.
2. Data backup and storage—centralized or decentralized approach.

3. Timely application of system patches—part of configuration management.
4. Access control measures.
5. Network infrastructure protection measures.

5.2.2 LASO Training

LASO training shall be required prior to assuming duties but no later than six months after initial assignment, and annually thereafter.

At a minimum, the following topics shall be addressed as enhanced security awareness training for a LASO:

1. The roles and responsibilities listed in CJIS Security Policy Section 3.2.9.
2. Additional state/local/tribal/federal agency LASO roles and responsibilities.
3. Summary of audit findings from previous state audits of local agencies.
4. Findings from the last FBI CJIS Division audit of the CSA.
5. Most recent changes to the CJIS Security Policy.

5.2.3 Security Training Records

Records of individual basic security awareness training and specific information system security training shall be documented, kept current, and maintained by the CSO/SIB Chief/Compact Officer. Maintenance of training records can be delegated to the local level.

Figure 4 – Security Awareness Training Use Cases

Use Case 1 - Security Awareness Training Program Implementation by a Local Police Department

A local police department with a staff of 20 sworn criminal justice professionals and 15 support personnel worked with a vendor to develop role-specific security-awareness training, and required all staff to complete this training upon assignment and every two years thereafter. The local police department scheduled the sworn law-enforcement training to coincide with their NCIC certification training. The vendor maintained the training records for the police department's entire staff, and provided reporting to the department to help it ensure compliance with the CJIS Security Policy.

Use Case 2 - Level One Security Awareness Training

A local police department hires custodial staff that will have physical access throughout the PD (a physically secure location) after normal business hours to clean the facility. These personnel have unescorted access to a physically secure location and therefore must be given the baseline security awareness training on all the topics identified in CSP Section 5.2.1.1 Level One Security Awareness Training.

Use Case 3 – Level Two Security Awareness Training

A school district maintains a locked file cabinet with hard copies of background check results of all teachers and employees which may include CJI (CHRI). Only authorized personnel who have the

ability to open the cabinet are required to be given the baseline security awareness training on all the topics identified in CSP Sections 5.2.1.1 and 5.2.1.2.

Use Case 4 – Level Three Security Awareness Training

A County Sheriff's Office has employed a number of dispatchers. Part of the function of these dispatchers is to run CJI queries at the request of the Sheriff and deputies. As part of their daily duties, the dispatchers have access to CJI both logically (running queries) and physically (printed copies of reports containing CJI). These dispatchers are entrusted with direct access to CJI and are therefore required to be given the baseline security awareness training on all the topics identified in CSP Sections 5.2.1.1, 5.2.1.2, and 5.2.1.3.

Use Case 5 – Level Four Security Awareness Training

The State Police has hired a number of system and network administrator personnel to help bolster security of the state network. Part of their daily duties may include creating accounts for new personnel, implementing security patches for existing systems, creating backups of existing systems, and implementing access controls throughout the network. These administrators have privileged access to CJI and CJI-processing systems, and are therefore required to be given the baseline security awareness training on all the topics identified in CSP Sections 5.2.1.1, 5.2.1.2, 5.2.1.3, and 5.2.1.4.

5.3 Policy Area 3: Incident Response

The security risk of both accidental and malicious attacks against government and private agencies, remains persistent in both physical and logical environments. To ensure protection of CJI, agencies shall: (i) establish operational incident handling procedures that include adequate preparation, detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities.

ISOs have been identified as the POC on security-related issues for their respective agencies and shall ensure LASOs institute the CSA incident response reporting procedures at the local level. Appendix F contains a sample incident notification letter for use when communicating the details of a CJI-related incident to the FBI CJIS ISO.

Refer to Section 5.13.5 for additional incident response requirements related to mobile devices used to access CJI.

5.3.1 Reporting Security Events

The agency shall promptly report incident information to appropriate authorities. Security events, including identified weaknesses associated with the event, shall be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the agency shall employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors and third party users shall be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any security events and weaknesses as quickly as possible to the designated point of contact.

5.3.1.1 Reporting Structure and Responsibilities

5.3.1.1.1 FBI CJIS Division Responsibilities

The FBI CJIS Division shall:

1. Manage and maintain the CJIS Division's Computer Security Incident Response Capability (CSIRC).
2. Serve as a central clearinghouse for all reported intrusion incidents, security alerts, bulletins, and other security-related material.
3. Ensure additional resources for all incidents affecting FBI CJIS Division controlled systems as needed.
4. Disseminate prompt advisories of system threats and operating system vulnerabilities via the security policy resource center on FBI.gov, to include but not limited to: Product Security Bulletins, Virus Bulletins, and Security Clips.
5. Track all reported incidents and/or trends.
6. Monitor the resolution of all incidents.

5.3.1.1.2 CSA ISO Responsibilities

The CSA ISO shall:

1. Assign individuals in each state, federal, and international law enforcement organization to be the primary point of contact for interfacing with the FBI CJIS Division concerning incident handling and response.
2. Identify individuals who are responsible for reporting incidents within their area of responsibility.
3. Collect incident information from those individuals for coordination and sharing among other organizations that may or may not be affected by the incident.
4. Develop, implement, and maintain internal incident response procedures and coordinate those procedures with other organizations that may or may not be affected.
5. Collect and disseminate all incident-related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement POCs within their area.
6. Act as a single POC for their jurisdictional area for requesting incident response assistance.

5.3.2 Management of Security Incidents

A consistent and effective approach shall be applied to the management of security incidents. Responsibilities and procedures shall be in place to handle security events and weaknesses effectively once they have been reported.

5.3.2.1 Incident Handling

The agency shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. Wherever feasible, the agency shall employ automated mechanisms to support the incident handling process.

Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The agency should incorporate the lessons learned from ongoing incident handling activities into the incident response procedures and implement the procedures accordingly.

5.3.2.2 Collection of Evidence

Where a follow-up action against a person or agency after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

5.3.3 Incident Response Training

The agency shall ensure general incident response roles responsibilities are included as part of required security awareness training.

5.3.4 Incident Monitoring

The agency shall track and document security incidents on an ongoing basis. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.

Figure 5 – Incident Response Process Initiated by an Incident in a Local Police Department

A state ISO received a notification from a local police department that suspicious network activity from a known botnet was detected on their network. The state ISO began the process of collecting all pertinent information about this incident, e.g. incident date/time, points-of-contact, systems affected, nature of the incident, actions taken, etc. and requested that the local police department confirm that their malware signatures were up to date. The state ISO contacted both the FBI CJIS ISO and state CSO to relay the preliminary details of this incident. The FBI CJIS ISO instructed the involved parties to continue their investigation and to submit an incident response form once all the information had been gathered. The FBI CJIS ISO contacted the lead for the FBI CSIRC to inform them that an incident response form was forthcoming. The state ISO gathered the remainder of the information from the local police department and submitted a completed incident response form to the FBI CJIS ISO who subsequently provided it to the FBI CSIRC. The FBI CSIRC notified the Department of Justice Computer Incident Response Team (DOJCIRT). The state ISO continued to monitor the situation, passing relevant details to the FBI CJIS ISO, ultimately determining that the botnet was eliminated from the local police department's infrastructure. Subsequent investigations determined that the botnet was restricted to the department's administrative infrastructure and thus no CJI was compromised.

5.4 Policy Area 4: Auditing and Accountability

Agencies shall implement audit and accountability controls to increase the probability of authorized users conforming to a prescribed pattern of behavior. Agencies shall carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components.

Auditing controls are typically applied to the components of an information system that provide auditing capability (servers, etc.) and would not necessarily be applied to every user-level workstation within the agency. As technology advances, more powerful and diverse functionality can be found in such devices as personal digital assistants and cellular telephones, which may require the application of security controls in accordance with an agency assessment of risk.

Refer to Section 5.13.6 for additional audit requirements related to mobile devices used to access CJI.

5.4.1 Auditable Events and Content (Information Systems)

The agency's information system shall generate audit records for defined events. These defined events include identifying significant events which need to be audited as relevant to the security of the information system. The agency shall specify which information system components carry out auditing activities. Auditing activity can affect information system performance and this issue must be considered as a separate factor during the acquisition of information systems.

The agency's information system shall produce, at the application and/or operating system level, audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. The agency shall periodically review and update the list of agency-defined auditable events. In the event an agency does not use an automated system, manual recording of activities shall still take place.

5.4.1.1 Events

The following events shall be logged:

1. Successful and unsuccessful system log-on attempts.
2. Successful and unsuccessful attempts to use:
 - a. access permission on a user account, file, directory or other system resource;
 - b. create permission on a user account, file, directory or other system resource;
 - c. write permission on a user account, file, directory or other system resource;
 - d. delete permission on a user account, file, directory or other system resource;
 - e. change permission on a user account, file, directory or other system resource.
3. Successful and unsuccessful attempts to change account passwords.
4. Successful and unsuccessful actions by privileged accounts (i.e. root, Oracle, DBA, admin, etc.).
5. Successful and unsuccessful attempts for users to:
 - a. access the audit log file;

- b. modify the audit log file;
- c. destroy the audit log file.

5.4.1.1.1 Content

The following content shall be included with every audited event:

1. Date and time of the event.
2. The component of the information system (e.g., software component, hardware component) where the event occurred.
3. Type of event.
4. User/subject identity.
5. Outcome (success or failure) of the event.

5.4.2 Response to Audit Processing Failures

The agency's information system shall provide alerts to appropriate agency officials in the event of an audit processing failure. Audit processing failures include, for example: software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

5.4.3 Audit Monitoring, Analysis, and Reporting

The responsible management official shall designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions. Audit review/analysis shall be conducted at a minimum once a week. The frequency of review/analysis should be increased when the volume of an agency's processing indicates an elevated need for audit review. The agency shall increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to agency operations, agency assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

5.4.4 Time Stamps

The agency's information system shall provide time stamps for use in audit record generation. The time stamps shall include the date and time values generated by the internal system clocks in the audit records. The agency shall synchronize internal information system clocks on an annual basis.

5.4.5 Protection of Audit Information

The agency's information system shall protect audit information and audit tools from modification, deletion and unauthorized access.

5.4.6 Audit Record Retention

The agency shall retain audit records for at least one (1) year. Once the minimum retention time period has passed, the agency shall continue to retain audit records until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for

example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.

5.4.7 Logging NCIC and III Transactions

A log shall be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log shall clearly identify both the operator and the authorized receiving agency. III logs shall also clearly identify the requester and the secondary recipient. The identification on the log shall take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one year retention period.

Figure 6 – Local Police Department's Use of Audit Logs

A state CSO contacted a local police department regarding potentially inappropriate use of CHRI that was retrieved using the local department's ORI. The state CSO requested all relevant information from the police department to reconcile state NCIC and III logs against local police department logs. The police department provided the combination of their CJI processing application's logs with relevant operating system and network infrastructure logs to help verify the identity of the users conducting these queries. The review of these logs substantiated the CSO's suspicion.

5.5 Policy Area 5: Access Control

Access control provides the planning and implementation of mechanisms to restrict reading, writing, processing and transmission of CJIS information and the modification of information systems, applications, services and communication configurations allowing access to CJIS information.

Refer to Section 5.13.6 for additional access control requirements related to mobile devices used to access CJI.

5.5.1 Account Management

The agency shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The agency shall validate information system accounts at least annually and shall document the validation process. The validation and documentation of accounts can be delegated to local agencies.

Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The agency shall identify authorized users of the information system and specify access rights/privileges. The agency shall grant access to the information system based on:

1. Valid need-to-know/need-to-share that is determined by assigned official duties.
2. Satisfaction of all personnel security criteria.

The agency responsible for account creation shall be notified when:

1. A user's information system usage or need-to-know or need-to-share changes.
2. A user is terminated or transferred or associated accounts are removed, disabled, or otherwise secured.

5.5.2 Access Enforcement

The information system shall enforce assigned authorizations for controlling access to the system and contained information. The information system controls shall restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.

Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users with access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers).

Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) shall be employed by agencies to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system.

5.5.2.1 Least Privilege

The agency shall approve individual access privileges and shall enforce physical and logical access restrictions associated with changes to the information system; and generate, retain, and review records reflecting all such changes. The agency shall enforce the most restrictive set of rights/privileges or access needed by users for the performance of specified tasks. The agency shall implement least privilege based on specific duties, operations, or information systems as necessary to mitigate risk to CJI. This limits access to CJI to only authorized personnel with the need and the right to know.

Logs of access privilege changes shall be maintained for a minimum of one year or at least equal to the agency's record retention policy – whichever is greater.

5.5.2.2 System Access Control

Access control mechanisms to enable access to CJI shall be restricted by object (e.g., data set, volumes, files, records) including the ability to read, write, or delete the objects. Access controls shall be in place and operational for all IT systems to:

1. Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the agency grants authority based upon operational business needs. Agencies shall document the parameters of the operational business needs for multiple concurrent active sessions.
2. Ensure that only authorized personnel can add, change, or remove component devices, dial-up connections, and remove or alter programs.

5.5.2.3 Access Control Criteria

Agencies shall control access to CJI based on one or more of the following:

1. Job assignment or function (i.e., the role) of the user seeking access.
2. Physical location.
3. Logical location.
4. Network addresses (e.g., users from sites within a given agency may be permitted greater access than those from outside).
5. Time-of-day and day-of-week/month restrictions.

5.5.2.4 Access Control Mechanisms

When setting up access controls, agencies shall use one or more of the following mechanisms:

1. Access Control Lists (ACLs). ACLs are a register of users (including groups, machines, processes) who have been given permission to use a particular object (system resource) and the types of access they have been permitted.
2. Resource Restrictions. Access to specific functions is restricted by never allowing users to request information, functions, or other resources for which they do not have access. Three major types of resource restrictions are: menus, database views, and network devices.

3. Encryption. Encrypted information can only be decrypted, and therefore read, by those possessing the appropriate cryptographic key. While encryption can provide strong access control, it is accompanied by the need for strong key management. Follow the guidance in Section 5.10.1.2 for encryption requirements if encryption of stored information is employed as an access enforcement mechanism.
4. Application Level. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level to provide increased information security for the agency.

5.5.3 Unsuccessful Login Attempts

Where technically feasible, the system shall enforce a limit of no more than 5 consecutive invalid access attempts by a user (attempting to access CJI or systems with access to CJI). The system shall automatically lock the account/node for a 10 minute time period unless released by an administrator.

5.5.4 System Use Notification

The information system shall display an approved system use notification message, before granting access, informing potential users of various usages and monitoring rules. The system use notification message shall, at a minimum, provide the following information:

1. The user is accessing a restricted information system.
2. System usage may be monitored, recorded, and subject to audit.
3. Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties.
4. Use of the system indicates consent to monitoring and recording.

The system use notification message shall provide appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remain on the screen until the user acknowledges the notification and takes explicit actions to log on to the information system.

Privacy and security policies shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. For publicly accessible systems:

1. the system use information is available and when appropriate, is displayed before granting access;
2. any references to monitoring, recording, or auditing are in keeping with privacy accommodations for such systems that generally prohibit those activities; and
3. the notice given to public users of the information system includes a description of the authorized uses of the system.

5.5.5 Session Lock

The information system shall prevent further access to the system by initiating a session lock after a maximum of 30 minutes of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures. Users shall

directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended. A session lock is not a substitute for logging out of the information system. In the interest of safety, devices that are: (1) part of a criminal justice conveyance; or (2) used to perform dispatch functions and located within a physically secure location; or (3) terminals designated solely for the purpose of receiving alert notifications (i.e. receive only terminals or ROT) used within physically secure location facilities that remain staffed when in operation, are exempt from this requirement. Note: an example of a session lock is a screen saver with password.

5.5.6 Remote Access

The agency shall authorize, monitor, and control all methods of remote access to the information system. Remote access is any temporary access to an agency's information system by a user (or an information system) communicating temporarily through an external, non-agency-controlled network (e.g., the Internet).

The agency shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. The agency shall control all remote accesses through managed access control points. The agency may permit remote access for privileged functions only for compelling operational needs but shall document the technical and administrative process for enabling remote access for privileged functions in the security plan for the information system.

Virtual escorting of privileged functions is permitted only when all the following conditions are met:

1. The session shall be monitored at all times by an authorized escort
2. The escort shall be familiar with the system/area in which the work is being performed.
3. The escort shall have the ability to end the session at any time.
4. The remote administrative personnel connection shall be via an encrypted (FIPS 140-2 certified) path.
5. The remote administrative personnel shall be identified prior to access and authenticated prior to or during the session. This authentication may be accomplished prior to the session via an Advanced Authentication (AA) solution or during the session via active teleconference with the escort throughout the session.

5.5.6.1 Personally Owned Information Systems

A personally owned information system shall not be authorized to access, process, store or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned information system usage. When personally owned mobile devices (i.e. bring your own device [BYOD]) are authorized, they shall be controlled in accordance with the requirements in Policy Area 13: Mobile Devices.

This control does not apply to the use of personally owned information systems to access agency's information systems and information that are intended for public access (e.g., an agency's public website that contains purely public information).

5.5.6.2 Publicly Accessible Computers

Publicly accessible computers shall not be used to access, process, store or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

Figure 7 – A Local Police Department's Access Controls

A local police department purchased a new computer-assisted dispatch (CAD) system that integrated with their state CSA's CJI interfaces. In doing so, the police department employed least-privilege practices to ensure that its employees were only given those privileges needed to perform their jobs, and as such, excluding IT administrators, employees had only non-administrative privileges on all equipment they used. The police department also used ACLs in the operating systems to control access to the CAD client's executables. The CAD system used internal role-based access controls to ensure only those users that needed access to CJI were given it. The police department performed annual audits of user accounts on all systems under their control including remote access mechanisms, operating systems, and the CAD system to ensure all accounts were in valid states. The police department implemented authentication-failure account lockouts, system use notification via login banners, and screen-saver passwords on all equipment that processes CJI.

5.6 Policy Area 6: Identification and Authentication

The agency shall identify information system users and processes acting on behalf of users and authenticate the identities of those users or processes as a prerequisite to allowing access to agency information systems or services.

5.6.1 Identification Policy and Procedures

Each person who is authorized to store, process, and/or transmit CJI shall be uniquely identified. A unique identification shall also be required for all persons who administer and maintain the system(s) that access CJI or networks leveraged for CJI transit. The unique identification can take the form of a full name, badge number, serial number, or other unique alphanumeric identifier. Agencies shall require users to identify themselves uniquely before the user is allowed to perform any actions on the system. Agencies shall ensure that all user IDs belong to currently authorized users. Identification data shall be kept current by adding new users and disabling and/or deleting former users.

5.6.1.1 Use of Originating Agency Identifiers in Transactions and Information Exchanges

An FBI authorized originating agency identifier (ORI) shall be used in each transaction on CJIS systems in order to identify the sending agency and to ensure the proper level of access for each transaction. The original identifier between the requesting agency and the CSA/SIB/Channeler shall be the ORI, and other agency identifiers, such as user identification or personal identifier, an access device mnemonic, or the Internet Protocol (IP) address.

Agencies may act as a servicing agency and perform transactions on behalf of authorized agencies requesting the service. Servicing agencies performing inquiry transactions on behalf of another agency may do so using the requesting agency's ORI. Servicing agencies may also use their own ORI to perform inquiry transactions on behalf of a requesting agency if the means and procedures are in place to provide an audit trail for the current specified retention period. Because the agency performing the transaction may not necessarily be the same as the agency requesting the transaction, the CSA/SIB/Channeler shall ensure that the ORI for each transaction can be traced, via audit trail, to the specific agency which is requesting the transaction.

Audit trails can be used to identify the requesting agency if there is a reason to inquire into the details surrounding why an agency ran an inquiry on a subject. Agencies assigned a P (limited access) ORI shall not use the full access ORI of another agency to conduct an inquiry transaction.

5.6.2 Authentication Policy and Procedures

Authentication refers to mechanisms or processes that verify users are valid once they are uniquely identified. The CSA/SIB may develop an authentication strategy which centralizes oversight but decentralizes the establishment and daily administration of the security measures for access to CJI.

Each individual's identity shall be authenticated at either the local agency, CSA, SIB or Channeler level. The authentication strategy shall be part of the agency's audit for policy compliance. The FBI CJIS Division shall identify and authenticate all individuals who establish direct web-based interactive sessions with FBI CJIS Services. The FBI CJIS Division shall authenticate the ORI of all message-based sessions between the FBI CJIS Division and its customer agencies but will not

further authenticate the user nor capture the unique identifier for the originating operator because this function is performed at the local agency, CSA, SIB or Channeler level.

5.6.2.1 Standard Authenticators

Authenticators are (the something you know, something you are, or something you have) part of the identification and authentication process. Examples of standard authenticators include passwords, hard or soft tokens, biometrics, one-time passwords (OTP) and personal identification numbers (PIN). Users shall not be allowed to use the same password or PIN in the same logon sequence.

5.6.2.1.1 Password

When agencies use a password as an authenticator for an individual's unique ID, they shall use the basic password standards in 5.6.2.1.1.1, OR follow the advanced password standards in 5.6.2.1.1.2.

NOTE: There is no option to combine or select particular options between the two separate lists below.

5.6.2.1.1.1 Basic Password Standards

When agencies elect to follow the basic password standards, passwords shall:

1. Be a minimum length of eight (8) characters on all systems.
2. Not be a dictionary word or proper name.
3. Not be the same as the Userid.
4. Expire within a maximum of 90 calendar days.
5. Not be identical to the previous ten (10) passwords.
6. Not be transmitted in the clear outside the secure location.
7. Not be displayed when entered.

5.6.2.1.1.2 Advanced Password Standards

When agencies elect to follow the advanced password standards, follow the guidance below:

1. Passwords shall be a minimum of twenty (20) characters in length with no additional complexity requirements imposed (e.g., ASCII characters, emojis, all keyboard characters, and spaces will be acceptable).
2. Password Verifiers shall not permit the use of a stored "hint" for forgotten passwords and/or prompt subscribers to use specific types of information (e.g., "What was the name of your first pet?") when choosing a password.
3. Verifiers shall maintain a list of "banned passwords" that contains values known to be commonly-used, expected, or compromised. For example, the list may include, but is not limited to:

- a. Passwords obtained from previous breach corpuses
 - b. Dictionary words
 - c. Repetitive or sequential characters (e.g. 'aaaaaa', '1234abcd')
 - d. Context-specific words, such as the name of the service, the username, and derivatives thereof
4. When processing requests to establish and change passwords, Verifiers shall compare the prospective passwords against the "banned passwords" list.
5. If the chosen password is found to be part of a "banned passwords" list, the Verifier shall:
 - a. Advise the subscriber that they need to select a different password,
 - b. Provide the reason for rejection, and
 - c. Require the subscriber to choose a different password.
6. Verifiers shall limit the number of failed authentication attempts that can be made as described in Section 5.5.3 Unsuccessful Login Attempts.
7. Verifiers shall force a password change if there is evidence of authenticator compromise or every 365 days from the last password change.
8. Verifiers shall use approved encryption and an authenticated protected channel when requesting passwords to protect against eavesdropping and Man-in-the-Middle (MitM) attacks.
9. Verifiers shall store passwords in a manner that is resistant to offline attacks by salting and hashing the password using a one-way key derivation function when stored.
 - a. The salt shall be at least 32 bits in length.
 - b. The salt shall be chosen arbitrarily so as to minimize salt value collisions among stored hashes.

Note: Key derivation functions take a password, a salt, and a cost factor as inputs then generate a password hash. Their purpose is to make each password guessing trial by an attacker who has obtained a password hash file expensive and therefore the cost of a guessing attack high or prohibitive.
10. For each subscriber, Verifiers shall protect stored salt and resulting hash values using a password or PIN.

5.6.2.1.2 Personal Identification Number (PIN)

When agencies implement the use of a PIN as a standard authenticator, the PIN attributes shall follow the guidance in section 5.6.2.1.1 (password). When agencies utilize a PIN in conjunction with a certificate or a token (e.g. key fob with rolling numbers) for the purpose of advanced authentication, agencies shall follow the PIN attributes described below. For example: A user certificate is installed on a smartphone for the purpose of advanced authentication (AA). As the user invokes that certificate, a PIN meeting the below attributes shall be used to access the certificate for the AA process.

1. Be a minimum of six (6) digits
2. Have no repeating digits (i.e., 112233)
3. Have no sequential patterns (i.e., 123456)
4. Not be the same as the Userid.
5. Expire within a maximum of 365 calendar days.
 - a. If a PIN is used to access a soft certificate which is the second factor of authentication, AND the first factor is a password that complies with the requirements in Section 5.6.2.1.1, then the 365 day expiration requirement can be waived by the CSO.
6. Not be identical to the previous three (3) PINs.
7. Not be transmitted in the clear outside the secure location.
8. Not be displayed when entered.

EXCEPTION: When a PIN is used for local device authentication, the only requirement is that it be a minimum of six (6) digits.

5.6.2.1.3 One-time Passwords (OTP)

One-time passwords are considered a “something you have” token for authentication. Examples include bingo cards, hard or soft tokens, and out-of-band tokens (i.e. OTP received via a text message).

When agencies implement the use of an OTP as an authenticator, the OTP shall meet the requirements described below.

1. Be a minimum of six (6) randomly generated characters
2. Be valid for a single session
3. If not used, expire within a maximum of five (5) minutes after issuance

5.6.2.2 Advanced Authentication

Advanced Authentication (AA) provides for additional security to the typical user identification and authentication of login ID and password, such as: biometric systems, user-based digital certificates (e.g. public key infrastructure (PKI)), smart cards, software tokens, hardware tokens, paper (inert) tokens, out-of-band authenticators (retrieved via a separate communication service channel – e.g., authenticator is sent on demand via text message, phone call, etc.), or “Risk-based Authentication” that includes a software token element comprised of a number of factors, such as

network information, user information, positive device identification (i.e. device forensics, user pattern analysis and user binding), user profiling, and high-risk challenge/response questions.

When user-based certificates are used for authentication purposes, they shall:

1. Be specific to an individual user and not to a particular device.
2. Prohibit multiple users from utilizing the same certificate.
3. Require the user to “activate” that certificate for each use in some manner (e.g., passphrase or user-specific PIN).

5.6.2.2.1 Advanced Authentication Policy and Rationale

The requirement to use or not use AA is dependent upon the physical, personnel, and technical security controls associated with the user location and whether CJI is accessed directly or indirectly. AA shall not be required for users requesting access to CJI from within the perimeter of a physically secure location (Section 5.9), when the technical security controls have been met (Sections 5.5 and 5.10), or when the user has no ability to conduct transactional activities on state and national repositories, applications, or services (i.e. indirect access). Conversely, if the technical security controls have not been met, AA shall be required even if the request for CJI originates from within a physically secure location. Section 5.6.2.2.2 provides agencies with a decision tree to help guide AA decisions. The CSO will make the final determination of whether access is considered indirect.

The intent of AA is to meet the standards of two-factor authentication. Two-factor authentication employs the use of two of the following three factors of authentication: something you know (e.g. password), something you have (e.g. hard token), something you are (e.g. biometric). The two authentication factors shall be unique (i.e. password/token or biometric/password but not password/password or token/token).

EXCEPTION:

AA shall be required when the requested service has built AA into its processes and requires a user to provide AA before granting access. EXAMPLES:

1. A user, irrespective of his/her location, accesses the LBBP portal. The LBBP has AA built into its services and requires AA prior to granting access. AA is required.
2. A user, irrespective of their location, accesses a State’s portal through which access to CJI is facilitated. The State Portal has AA built into its processes and requires AA prior to granting access. AA is required.

5.6.2.2.2 Advanced Authentication Decision Tree

The following AA Decision Tree, coupled with figures 9 and 10 below, assists decision makers in determining whether or not AA is required.

1. Can request’s physical originating location be determined?
If either (a) or (b) below are true the answer to the above question is “yes”. Proceed to question 2.
 - a. The IP address is attributed to a physical structure; or

- b. The mnemonic is attributed to a specific device assigned to a specific location that is a physical structure.

If neither (a) or (b) above are true then the answer is “no”. Skip to question number 4.

- 2. Does request originate from within a physically secure location as described in Section 5.9.1?

If either (a) or (b) below are true the answer to the above question is “yes”. Proceed to question 3.

- a. The IP address is attributed to a physically secure location; or
- b. If a mnemonic is used it is attributed to a specific device assigned to a specific physically secure location.

If neither (a) or (b) above are true then the answer is “no”. Decision tree completed. AA required.

- 3. Are all required technical controls implemented at this location or at the controlling agency?

If either (a) or (b) below are true the answer to the above question is “yes”. Decision tree completed. AA requirement waived.

- a. Appropriate technical controls listed in Sections 5.5 and 5.10 are implemented; or
- b. The controlling agency (i.e. parent agency or agency leveraged as conduit to CJI) extends its wide area network controls down to the requesting agency and the extended controls provide assurance equal or greater to the controls listed in Sections 5.5 and 5.10.

If neither (a) or (b) above are true then the answer is “no”. Decision tree completed. AA required.

- 4. Does request originate from an agency-controlled user device?

If either (a) or (b) below are true the answer to the above question is “yes”. Proceed to question 5.

- a. The static IP address or MAC address can be traced to registered device; or
- b. Certificates are issued to agency managed devices only and certificate exchange is allowed only between authentication server and agency issued devices.

If neither (a) or (b) above are true then the answer is “no”. Decision tree completed. AA required.

- 5. Is the agency managed user device associated with and located within a criminal justice conveyance?

If any of the (a), (b), or (c) statements below is true the answer to the above question is “yes”. Proceed to Figure 9 Step 3.

- a. The static IP address or MAC address is associated with a device associated with a criminal justice conveyance; or

- b. The certificate presented is associated with a device associated with a criminal justice conveyance; or
- c. The mnemonic presented is associated with a specific device assigned and that device is attributed to a criminal justice conveyance.

If none of the (a), (b), or (c) statements above are true then the answer is “no”. Skip to question number 7.

6. Is the user device an agency-issued and controlled smartphone or tablet?

If both (a) and (b) below are true, the answer to the above question is “yes.” Proceed to question number 7.

- a. The law enforcement agency issued the device to an individual; and
- b. The device is subject to administrative management control of the issuing agency.

If either (a) or (b) above is false, then the answer is “no.” Decision tree completed. AA required.

7. Does the agency-issued smartphone or tablet have CSO-approved AA compensating controls implemented?

If (a) and (b) below are true, the answer to the above question is “yes.” Decision tree completed. AA requirement is waived.

- a. An agency cannot meet a requirement due to legitimate technical or business constraints; and
- b. The CSO has given written approval permitting AA compensating controls to be implemented in lieu of the required AA control measures.

If either (a) or (b) above is false then the answer is “no.” Decision tree completed. AA required.

5.6.3 Identifier and Authenticator Management

The agency shall establish identifier and authenticator management processes.

5.6.3.1 Identifier Management

In order to manage user identifiers, agencies shall:

1. Uniquely identify each user.
2. Verify the identity of each user.
3. Receive authorization to issue a user identifier from an appropriate agency official.
4. Issue the user identifier to the intended party.
5. Disable the user identifier after a specified period of inactivity.
6. Archive user identifiers.

5.6.3.2 Authenticator Management

In order to manage information system authenticators, agencies shall:

1. Define initial authenticator content.
2. Establish administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators.
3. Change default authenticators upon information system installation.
4. Change/refresh authenticators periodically.

Information system authenticators include, for example, tokens, user-based PKI certificates, biometrics, passwords, and key cards. Users shall take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and immediately reporting lost or compromised authenticators.

5.6.4 Assertions

Identity providers can be leveraged to identify individuals and assert the individual's identity to a service or to a trusted broker who will in-turn assert the identity to a service. Assertion mechanisms used to communicate the results of a remote authentication to other parties shall be:

1. Digitally signed by a trusted entity (e.g., the identity provider).
2. Obtained directly from a trusted entity (e.g. trusted broker) using a protocol where the trusted entity authenticates to the relying party using a secure protocol (e.g. transport layer security [TLS]) that cryptographically authenticates the verifier and protects the assertion.

Assertions generated by a verifier shall expire after 12 hours and shall not be accepted thereafter by the relying party.

Figure 8 – Advanced Authentication Use Cases

Use Case 1 - A Local Police Department Authentication Control Scenario

During the course of an investigation, a detective attempts to access Criminal Justice Information (CJI) from a hotel room using an agency issued mobile broadband card. To gain access, the detective first establishes the remote session via a secure virtual private network (VPN) tunnel (satisfying the requirement for encryption). Upon connecting to the agency network, the detective is challenged for a username (identification), password ("something you know"), and a one-time password OTP ("something you have") from a hardware token to satisfy the requirement for advanced authentication. Once the detective's credentials are validated, his identity is asserted by the infrastructure to all authorized applications needed to complete his queries.

Use Case 2 – Use of a Smart Card

A user is issued a smart card that is loaded with user-specific digital certificates from a terminal within a controlled area. The user selects an application that will provide access to

Criminal Justice Information (CJI) then enters the proper username (identification) and password ("something you know"). Once prompted, the user connects the smart card ("something you have") to the terminal. The user is prompted to enter a personal identification number (PIN) to unlock the smart card. Once unlocked, the smart card sends the certificates to the authentication management server at the local agency where the combined username, password, and digital user certificates are validated. The user has satisfied the requirement for AA and is granted access to CJI.

Use Case 3 – Out of Band One-Time-Password (OTP) – Mobile phone-based

Using an agency- issued laptop, a user connects to the agency network via an agency-issued mobile broadband card and an encrypted virtual private network (VPN) tunnel. As part of an on-going investigation, the user initiates an application that will permit access to Criminal Justice Information (CJI). The user is prompted to enter a username (identification) and a password ("something you know"). Once that has been completed, a text message containing a one-time password (OTP) is sent via text message (out of band) to the user's agency-issued cell phone. The user is challenged via the CJI application for that OTP. The user enters the OTP ("something you have") then the username, password, and OTP are validated. The user has satisfied the requirement for AA and is granted access to CJI.

Use Case 4 – Improper Use of a One-Time-Password (OTP) – Laptop

Using an agency- issued laptop, a user connects to the agency network via an agency-issued mobile broadband card and an encrypted virtual private network (VPN) tunnel. As part of an on-going investigation, the user initiates an application that will permit access to Criminal Justice Information (CJI). The user is prompted to enter a username (identification) and a password ("something you know"). Once that has been completed, a one-time password (OTP) is sent to the user's agency-issued laptop (in band) via pop-up message. The user is challenged via the CJI application for that OTP; however, the delivery of the OTP to the device that is being used to access CJI (in band) defeats the purpose of the second factor. This method does not satisfy the requirement for AA, and therefore the user should not be granted access to CJI. See the below explanation:

This method of receiving the necessary OTP (in band) does not guarantee the authenticity of the user's identity because anyone launching the CJI application and entering a valid username/password combination is presented the OTP via a pop-up which is intend to be the second factor of authentication. This method makes the application accessible to anyone with knowledge of the valid username and password. Potentially, this is no more secure than using only a single factor of authentication.

Use Case 5 – Risk-based Authentication (RBA) Implementation

A user has moved office locations and requires email access (containing Criminal Justice Information) via an Outlook Web Access (OWA) client utilizes a risk-based authentication (RBA) solution. The user launches the OWA client and is prompted to enter a username

(identification) and a password (“something you know”). The RBA detects this computer has not previously been used by the user, is not listed under the user’s profile, and then presents high-risk challenge/response question(s) which the user is prompted to answer. Once the questions have been verified as correct, the user is authenticated and granted access to the email. Meanwhile, the RBA logs and collects a number of device forensic information and captures the user pattern analysis to update the user’s profile. The CJIS Security Policy requirements for RBA have been satisfied.

Use Case 6 – Improper Risk-based Authentication (RBA) Implementation

A user has moved office locations and requires access to email containing Criminal Justice Information (CJI) via an Outlook Web Access (OWA) client utilizing a risk-based authentication (RBA) solution. The user launches the OWA client and is prompted to enter a username (identification) and a password (“something you know”). The RBA detects this computer has not previously been used by the user and is not listed under the user’s profile. The user is prompted to answer high-risk challenge/response questions for verification and authorization to access to the email; however, if the second authentication factor is to answer additional questions presented every time the user logs on, then this solution is referred to as a knowledge-based authentic on (KBA) solution. A KBA solution does not satisfy the requirement for AA, and therefore the user should not be granted access to CJI.

See the below explanation:

A KBA solution is not a viable advanced authentication (AA) solution per the CJIS Security Policy (CSP). The KBA asks questions and compares the answers to those stored within the user’s profile. A KBA is neither a CSP compliant two factor authentication solution, nor does it meet the CSP criteria of a risk-based authentication (RBA) solution which logs and collects a number of device forensic information and captures the user pattern analysis to update the user’s profile. Using this collected data, the RBA presents challenge/response questions when changes to the user’s profile are noted versus every time the user logs in.

Use Case 7 – Advanced Authentication Compensating Controls on Agency-Issued Smartphones

An authorized user is issued a smartphone that is administratively managed by the agency-installed mobile device management (MDM) solution to ensure device compliance with the CJIS Security Policy. The user initiates an email client on the smartphone that contains emails with CJI. The email client challenges the user to enter a username (identification) and a password (one factor: something you know) which are forwarded to the local agency for authentication. The smartphone lacks the technical capability to challenge the user for a second factor of authentication. This email client is used across the state agency so access is a necessity for the user’s job functions.

An audit by the CSA identifies the agency’s use of the agency smartphone as not compliant with AA requirements due to the authorized user authenticating with only one factor instead of the required two factors.

Subsequently, the agency performs a risk assessment of their smartphone authentication solution and document a legitimate technical constraint due to the lack of technical solutions for smartphone-based two-factor authentication. The risk assessment identifies the following compensating controls that, when combined with the authorized user authenticating to the local agency with their password, meet the intent of the AA requirement by providing a similar level of security:

1. Enhance smartphone policy to enable possession of the smartphone to be considered a factor of authentication (i.e. something you have). Require authorized users to treat the smartphone as a controlled device and protect it as they would a personal credit card or an issued firearm to ensure only they will be in possession of the device
2. Move the email client used to authenticate with the local agency inside an encrypted, password-protected secure container on the smartphone ensuring only the authorized user can access the email application to authenticate.

The agency submits an AA compensating controls request to the CSO outlining the technical constraint identified by the risk assessment, what compensating controls will be employed, and the desired duration of the compensating controls.

The CSO approves the agency's request and provides documentation of the approval to the agency to maintain for audit purposes. The agency enacts the compensating controls and informs agency personnel they are permitted to access CJI via the agency-issued smartphone.

Figure 9 – Authentication Decision for Known Location

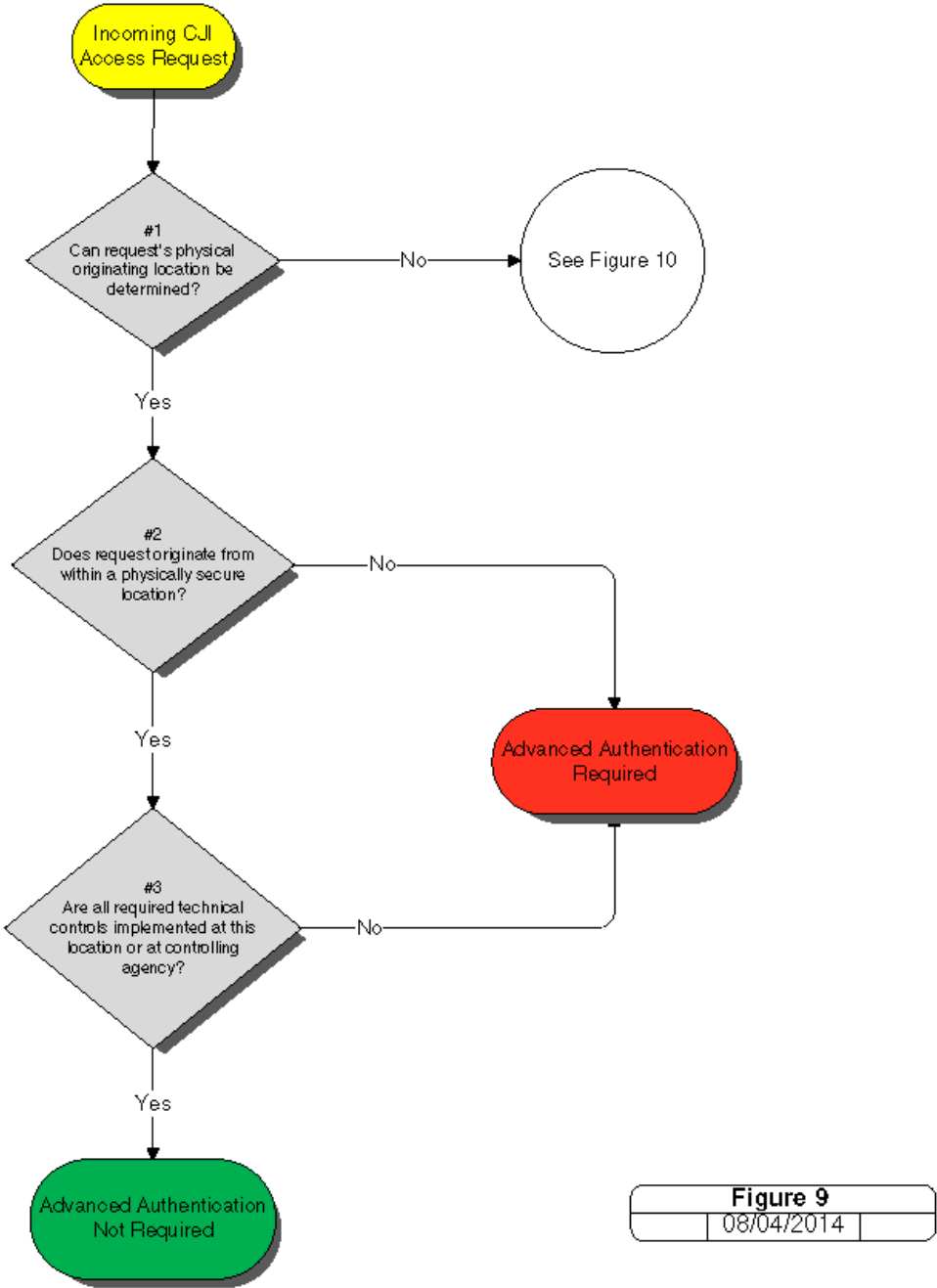


Figure 10 – Authentication Decision for Unknown Location

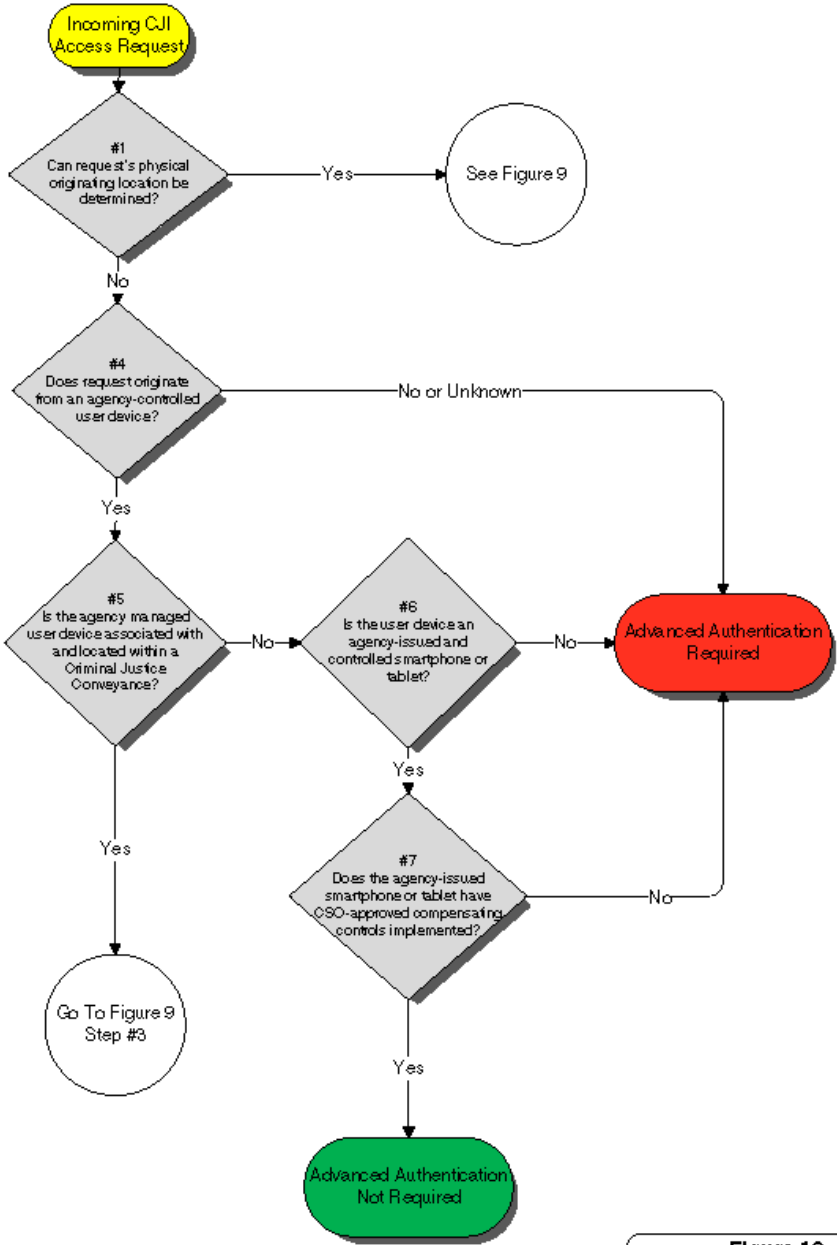


Figure 10		
	10/06/2015	

5.7 Policy Area 7: Configuration Management

5.7.1 Access Restrictions for Changes

Planned or unplanned changes to the hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system. The goal is to allow only qualified and authorized individuals access to information system components for purposes of initiating changes, including upgrades, and modifications. Section 5.5, Access Control, describes agency requirements for control of privileges and restrictions.

5.7.1.1 Least Functionality

The agency shall configure the application, service, or information system to provide only essential capabilities and shall specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.

5.7.1.2 Network Diagram

The agency shall ensure that a complete topological drawing depicting the interconnectivity of the agency network, to criminal justice information, systems and services is maintained in a current status. See Appendix C for sample network diagrams.

The network topological drawing shall include the following:

1. All communications paths, circuits, and other components used for the interconnection, beginning with the agency-owned system(s) and traversing through all interconnected systems to the agency end-point.
2. The logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Individual workstations (clients) do not have to be shown; the number of clients is sufficient.
3. "For Official Use Only" (FOUO) markings.
4. The agency name and date (day, month, and year) drawing was created or updated.

5.7.2 Security of Configuration Documentation

The system configuration documentation often contains sensitive details (e.g. descriptions of applications, processes, procedures, data structures, authorization processes, data flow, etc.) Agencies shall protect the system documentation from unauthorized access consistent with the provisions described in Section 5.5 Access Control.

Figure 11 – A Local Police Department's Configuration Management Controls

A local police department decided to update their CAD system, and in doing so tracked all changes made to their infrastructure in a configuration management journal, updated their network topology documents to include all new components in their architecture, then marked all documentation as FOUO and stored them securely.

5.8 Policy Area 8: Media Protection

Media protection policy and procedures shall be documented and implemented to ensure that access to digital and physical media in all forms is restricted to authorized individuals. Procedures shall be defined for securely handling, transporting and storing media.

5.8.1 Media Storage and Access

The agency shall securely store digital and physical media within physically secure locations or controlled areas. The agency shall restrict access to digital and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data shall be encrypted per Section 5.10.1.2.

5.8.2 Media Transport

The agency shall protect and control digital and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.

5.8.2.1 Digital Media during Transport

Controls shall be in place to protect digital media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in Section 5.10.1.2 of this Policy, is the optimal control during transport; however, if encryption of the data isn't possible then each agency shall institute physical controls to ensure the security of the data.

5.8.2.2 Physical Media in Transit

The controls and security measures in this document also apply to CJI in physical (printed documents, printed imagery, etc.) form. Physical media shall be protected at the same level as the information would be protected in electronic form.

5.8.3 Digital Media Sanitization and Disposal

The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

5.8.4 Disposal of Physical Media

Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.

Figure 12 – A Local Police Department’s Media Management Policies

A local police department implemented a replacement CAD system that integrated to their state’s CSA and was authorized to process CJI. The police department contracted with an off-site media manager to store backups of their data in the contractor’s vaults, but the contractor was not authorized to process or store CJI. To ensure the confidentiality of the police department’s data while outside its perimeter, they encrypted all data going to the contractor with an encryption product that is FIPS 140-2 certified. The police department rotated and reused media through the contractor’s vaults periodically, and when it required destruction, the police department incinerated the media to irreversibly destroy any data on it.

5.9 Policy Area 9: Physical Protection

Physical protection policy and procedures shall be documented and implemented to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

5.9.1 Physically Secure Location

A physically secure location is a facility, a criminal justice conveyance, or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. The physically secure location is subject to criminal justice agency management control; SIB control; FBI CJIS Security addendum; or a combination thereof.

Sections 5.9.1.1 – 5.9.1.8 describe the physical controls required in order to be considered a physically secure location, while Sections 5.2 and 5.12, respectively, describe the minimum security awareness training and personnel security controls required for unescorted access to a physically secure location. Sections 5.5, 5.6.2.2.1, and 5.10 describe the requirements for technical security controls required to access CJI from within the perimeter of a physically secure location without AA.

5.9.1.1 Security Perimeter

The perimeter of a physically secure location shall be prominently posted and separated from non-secure locations by physical controls. Security perimeters shall be defined, controlled and secured in a manner acceptable to the CSA or SIB.

5.9.1.2 Physical Access Authorizations

The agency shall develop and keep current a list of personnel with authorized access to the physically secure location (except for those areas within the permanent facility officially designated as publicly accessible) or shall issue credentials to authorized personnel.

5.9.1.3 Physical Access Control

The agency shall control all physical access points (except for those areas within the facility officially designated as publicly accessible) and shall verify individual access authorizations before granting access.

5.9.1.4 Access Control for Transmission Medium

The agency shall control physical access to information system distribution and transmission lines within the physically secure location.

5.9.1.5 Access Control for Display Medium

The agency shall control physical access to information system devices that display CJI and shall position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI.

5.9.1.6 Monitoring Physical Access

The agency shall monitor physical access to the information system to detect and respond to physical security incidents.

5.9.1.7 Visitor Control

The agency shall control physical access by authenticating visitors before authorizing escorted access to the physically secure location (except for those areas designated as publicly accessible). The agency shall escort visitors at all times and monitor visitor activity.

5.9.1.8 Delivery and Removal

The agency shall authorize and control information system-related items entering and exiting the physically secure location.

5.9.2 Controlled Area

If an agency cannot meet all of the controls required for establishing a physically secure location, but has an operational need to access or store CJI, the agency shall designate an area, a room, or a storage container, as a controlled area for the purpose of day-to-day CJI access or storage. The agency shall, at a minimum:

1. Limit access to the controlled area during CJI processing times to only those personnel authorized by the agency to access or view CJI.
2. Lock the area, room, or storage container when unattended.
3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.
4. Follow the encryption requirements found in Section 5.10.1.2 for electronic storage (i.e. data “at rest”) of CJI.

Figure 13 – A Local Police Department's Physical Protection Measures

A local police department implemented a replacement CAD system that was authorized to process CJI over an encrypted VPN tunnel to the state's CSA. The police department established a physically separated wing within their precinct separated by locked doors, walls, and a monitored security system within which CJI was processed by criminal justice professionals. Only those persons with the appropriate authorizations were permitted within this wing unless accompanied by such a person. Within this secure wing the police department further segregated the back-office information systems' infrastructure within a separately controlled area restricted only to those authorized administrative personnel with a need to enter.

5.10 Policy Area 10: System and Communications Protection and Information Integrity

Examples of systems and communications safeguards range from boundary and transmission protection to securing an agency's virtualized environment. In addition, applications, services, or information systems must have the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information. This section details the policy for protecting systems and communications infrastructures.

Refer to Section 5.13.4 for additional system integrity requirements related to mobile devices used to access CJI.

5.10.1 Information Flow Enforcement

The network infrastructure shall control the flow of information between interconnected systems. Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. In other words, controlling how data moves from one place to the next in a secure manner. Examples of controls that are better expressed as flow control than access control (see Section 5.5) are:

1. Prevent CJI from being transmitted unencrypted across the public network.
2. Block outside traffic that claims to be from within the agency.
3. Do not pass any web requests to the public network that are not from the internal web proxy.

Specific examples of flow control enforcement can be found in boundary protection devices (e.g. proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability.

5.10.1.1 Boundary Protection

The agency shall:

1. Control access to networks processing CJI.
2. Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.
3. Ensure any connections to the Internet, other external networks, or information systems occur through controlled interfaces (e.g. proxies, gateways, routers, firewalls, encrypted tunnels). See Section 5.13.4.3 for guidance on personal firewalls.
4. Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use.
5. Ensure the operational failure of the boundary protection mechanisms do not result in any unauthorized release of information outside of the information system boundary (i.e. the device "fails closed" vs. "fails open").

6. Allocate publicly accessible information system components (e.g. public Web servers) to separate sub networks with separate, network interfaces. Publicly accessible information systems residing on a virtual host shall follow the guidance in Section 5.10.3.2 to achieve separation.

5.10.1.2 Encryption

Encryption is a form of cryptology that applies a cryptographic operation to provide confidentiality of (sensitive) information. Decryption is the reversing of the cryptographic operation to convert the information back into a plaintext (readable) format. There are two main types of encryption: symmetric encryption and asymmetric encryption (also known as public key encryption). Hybrid encryption solutions do exist and use both asymmetric encryption for client/server certificate exchange – session integrity and symmetric encryption for bulk data encryption – data confidentiality.

5.10.1.2.1 Encryption for CJI in Transit

When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via encryption. When encryption is employed, the cryptographic module used shall be FIPS 140-2 certified and use a symmetric cipher key strength of at least 128 bit strength to protect CJI.

NOTE: Subsequent versions of approved cryptographic modules that are under current review for FIPS 140-2 compliancy can be used in the interim until certification is complete.

EXCEPTIONS:

1. See Sections 5.13.1.2.2 and 5.10.2.
2. Encryption shall not be required if the transmission medium meets all of the following requirements:
 - a. The agency owns, operates, manages, or protects the medium.
 - b. Medium terminates within physically secure locations at both ends with no interconnections between.
 - c. Physical access to the medium is controlled by the agency using the requirements in Sections 5.9.1 and 5.12.
 - d. Protection includes safeguards (e.g., acoustic, electric, electromagnetic, and physical) and if feasible countermeasures (e.g., alarms, notifications) to permit its use for the transmission of unencrypted information through an area of lesser classification or control.
 - e. With prior approval of the CSO.

Examples:

- A campus is completely owned and controlled by a criminal justice agency (CJA)
 - If line-of-sight between buildings exists where a cable is buried, encryption is not required.

- A multi-story building is completely owned and controlled by a CJA – If floors are physically secure or cable runs through non-secure areas are protected, encryption is not required.
- A multi-story building is occupied by a mix of CJAs and non-CJAs – If floors are physically secure or cable runs through the non-secure areas are protected, encryption is not required.

5.10.1.2.2 Encryption for CJI at Rest

When CJI is at rest (i.e. stored digitally) outside the boundary of the physically secure location, the data shall be protected via encryption. When encryption is employed, agencies shall either encrypt CJI in accordance with the standard in Section 5.10.1.2.1 above, or use a symmetric cipher that is FIPS 197 certified (AES) and at least 256 bit strength.

1. When agencies implement encryption on CJI at rest, the passphrase used to unlock the cipher shall meet the following requirements:
 - a. Be at least 10 characters
 - b. Not be a dictionary word.
 - c. Include at least one (1) upper case letter, one (1) lower case letter, one (1) number, and one (1) special character.
 - d. Be changed when previously authorized personnel no longer require access.
2. Multiple files maintained in the same unencrypted folder shall have separate and distinct passphrases. A single passphrase may be used to encrypt an entire folder or disk containing multiple files. All audit requirements found in Section 5.4.1 Auditable Events and Content (Information Systems) shall be applied.

NOTE: Commonly available encryption tools often use a key to unlock the cipher to allow data access; this key is called a passphrase. While similar to a password, a passphrase is not used for user authentication. Additionally, the passphrase contains stringent character requirements making it more secure and thus providing a higher level of confidence that the passphrase will not be compromised.

5.10.1.2.3 Public Key Infrastructure (PKI) Technology

For agencies using public key infrastructure (PKI) technology, the agency shall develop and implement a certificate policy and certification practice statement for the issuance of public key certificates used in the information system. Registration to receive a public key certificate shall:

1. Include authorization by a supervisor or a responsible official.
2. Be accomplished by a secure process that verifies the identity of the certificate holder.
3. Ensure the certificate is issued to the intended party.

5.10.1.3 Intrusion Detection Tools and Techniques

Intrusion detection systems are deployed inside a network to monitor events against a known set of parameters (i.e. malicious activity or policy violations) and make notification to the system of any event which violates any of those parameters. They are passive in nature, listening and

monitoring network traffic. There are mainly two types of IDS; network-based IDS (NIDS) and host-based IDS (HIDS).

Intrusion prevention systems are an IDS with the capability to respond to detected intrusions. They are normally deployed at the perimeter of a network, scanning traffic. Like detection systems, protection systems compare scanned traffic to defined normal parameters but unlike detection systems are able to take some type of immediate action to mitigate, or prevent, an event.

Agencies shall:

1. Implement network-based and/or host-based intrusion detection or prevention tools.
2. Maintain current intrusion detection or prevention signatures.
3. Monitor inbound and outbound communications for unusual or unauthorized activities.
4. Send individual intrusion detection logs to a central logging facility where correlation and analysis will be accomplished as a system wide intrusion detection effort.
5. Review intrusion detection or prevention logs weekly or implement automated event notification.
6. Employ automated tools to support near-real-time analysis of events in support of detecting system-level attacks.

5.10.1.4 Voice over Internet Protocol

Voice over Internet Protocol (VoIP) has been embraced by organizations globally as an addition to, or replacement for, public switched telephone network (PSTN) and private branch exchange (PBX) telephone systems. The immediate benefits are lower costs than traditional telephone services and VoIP can be installed in-line with an organization's existing Internet Protocol (IP) services. Among VoIP's risks that have to be considered carefully are: myriad security concerns, cost issues associated with new networking hardware requirements, and overarching quality of service (QoS) factors.

In addition to the security controls described in this document, the following additional controls shall be implemented when an agency deploys VoIP within a network that contains unencrypted CJI:

1. Establish usage restrictions and implementation guidance for VoIP technologies.
2. Change the default administrative password on the IP phones and VoIP switches.
3. Utilize Virtual Local Area Network (VLAN) technology to segment VoIP traffic from data traffic.

Appendix G.2 outlines threats, vulnerabilities, mitigations, and NIST best practices for VoIP.

5.10.1.5 Cloud Computing

Organizations transitioning to a cloud environment are presented unique opportunities and challenges (e.g., purported cost savings and increased efficiencies versus a loss of control over the data). Reviewing the cloud computing white paper (Appendix G.3), the cloud assessment located within the security policy resource center on FBI.gov, NIST Special Publications (800-144, 800-

145, and 800-146), as well as the cloud provider's policies and capabilities will enable organizations to make informed decisions on whether or not the cloud provider can offer service that maintains compliance with the requirements of the CJIS Security Policy.

The storage of CJI, regardless of encryption status, shall only be permitted in cloud environments (e.g. government or third-party/commercial datacenters, etc.) which reside within the physical boundaries of APB-member country (i.e. U.S., U.S. territories, Indian Tribes, and Canada) and legal authority of an APB-member agency (i.e. U.S. – federal/state/territory, Indian Tribe, or the Royal Canadian Mounted Police (RCMP)).

Note: This restriction does not apply to exchanges of CJI with foreign government agencies under international exchange agreements (i.e. the Preventing and Combating Serious Crime (PCSC) agreements, fugitive extracts, and exchanges made for humanitarian and criminal investigatory purposes in particular circumstances).

Metadata derived from unencrypted CJI shall be protected in the same manner as CJI and shall not be used for any advertising or other commercial purposes by any cloud service provider or other associated entity.

The agency may permit limited use of metadata derived from unencrypted CJI when specifically approved by the agency and its "intended use" is detailed within the service agreement. Such authorized uses of metadata may include, but are not limited to the following: spam and spyware filtering, data loss prevention, spillage reporting, transaction logs (events and content – similar to Section 5.4), data usage/indexing metrics, and diagnostic/syslog data.

5.10.2 Facsimile Transmission of CJI

CJI transmitted via a single or multi-function device over a standard telephone line is exempt from encryption requirements. CJI transmitted external to a physically secure location using a facsimile server, application or service which implements email-like technology, shall meet the encryption requirements for CJI in transit as defined in Section 5.10.

5.10.3 Partitioning and Virtualization

As resources grow scarce, agencies are increasing the centralization of applications, services, and system administration. Advanced software now provides the ability to create virtual machines that allows agencies to reduce the amount of hardware needed. Although the concepts of partitioning and virtualization have existed for a while, the need for securing the partitions and virtualized machines has evolved due to the increasing amount of distributed processing and federated information sources now available across the Internet.

5.10.3.1 Partitioning

The application, service, or information system shall separate user functionality (including user interface services) from information system management functionality.

The application, service, or information system shall physically or logically separate user interface services (e.g. public web pages) from information storage and management services (e.g. database management). Separation may be accomplished through the use of one or more of the following:

1. Different computers.

2. Different central processing units.
3. Different instances of the operating system.
4. Different network addresses.
5. Other methods approved by the FBI CJIS ISO.

5.10.3.2 Virtualization

Virtualization refers to a methodology of dividing the resources of a computer (hardware and software) into multiple execution environments. Virtualized environments are authorized for criminal justice and noncriminal justice activities. In addition to the security controls described in this Policy, the following additional controls shall be implemented in a virtual environment:

1. Isolate the host from the virtual machine. In other words, virtual machine users cannot access host files, firmware, etc.
2. Maintain audit logs for all virtual machines and hosts and store the logs outside the hosts' virtual environment.
3. Virtual Machines that are Internet facing (web servers, portal servers, etc.) shall be physically separate from Virtual Machines (VMs) that process CJI internally or be separated by a virtual firewall.
4. Drivers that serve critical functions shall be stored within the specific VM they service. In other words, do not store these drivers within the hypervisor, or host operating system, for sharing. Each VM is to be treated as an independent system – secured as independently as possible.

The following additional technical security controls shall be applied in virtual environments where CJI is comingled with non-CJI:

1. Encrypt CJI when stored in a virtualized environment where CJI is comingled with non-CJI or segregate and store unencrypted CJI within its own secure VM.
2. Encrypt network traffic within the virtual environment.

The following are additional technical security control best practices and should be implemented wherever feasible:

1. Implement IDS and/or IPS monitoring within the virtual environment.
2. Virtually or physically firewall each VM within the virtual environment to ensure that only allowed protocols will transact.
3. Segregate the administrative duties for the host.

Appendix G-1 provides some reference and additional back ground information on virtualization.

5.10.4 System and Information Integrity Policy and Procedures

5.10.4.1 Patch Management

The agency shall identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.

The agency (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) shall develop and implement a local policy that ensures prompt installation of newly released security relevant patches, service packs and hot fixes. Local policies should include such items as:

1. Testing of appropriate patches before installation.
2. Rollback capabilities when installing patches, updates, etc.
3. Automatic updates without individual user intervention.
4. Centralized patch management.

Patch requirements discovered during security assessments, continuous monitoring or incident response activities shall also be addressed expeditiously.

5.10.4.2 Malicious Code Protection

The agency shall implement malicious code protection that includes automatic updates for all systems with Internet access. Agencies with systems not connected to the Internet shall implement local procedures to ensure malicious code protection is kept current (i.e. most recent update available).

The agency shall employ virus protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses) at critical points throughout the network and on all workstations, servers and mobile computing devices on the network. The agency shall ensure malicious code protection is enabled on all of the aforementioned critical points and information systems and resident scanning is employed.

5.10.4.3 Spam and Spyware Protection

The agency shall implement spam and spyware protection.

The agency shall:

1. Employ spam protection mechanisms at critical information system entry points (e.g., firewalls, electronic mail servers, remote-access servers).
2. Employ spyware protection at workstations, servers and mobile computing devices on the network.
3. Use the spam and spyware protection mechanisms to detect and take appropriate action on unsolicited messages and spyware/adware, respectively, transported by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g. diskettes or compact disks) or other removable media as defined in this Policy.

5.10.4.4 Security Alerts and Advisories

The agency shall:

1. Receive information system security alerts/advisories on a regular basis.
2. Issue alerts/advisories to appropriate personnel.
3. Document the types of actions to be taken in response to security alerts/advisories.
4. Take appropriate actions in response.

5. Employ automated mechanisms to make security alert and advisory information available throughout the agency as appropriate.

5.10.4.5 Information Input Restrictions

The agency shall restrict the information input to any connection to FBI CJIS services to authorized personnel only.

Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.

Figure 14 – System and Communications Protection and Information Integrity Use Cases

Use Case 1 – A Local Police Department’s Information Systems & Communications Protections

A local police department implemented a replacement CAD system within a physically secure location that was authorized to process CJI using a FIPS 140-2 encrypted VPN tunnel over the Internet to the state’s CSA. In addition to the policies, physical and personnel controls already in place, the police department employed firewalls both at their border and at key points within their network, intrusion detection systems, a patch-management strategy that included automatic patch updates where possible, virus scanners, spam and spyware detection mechanisms that update signatures automatically, and subscribed to various security alert mailing lists and addressed vulnerabilities raised through the alerts as needed.

Use Case 2 – Faxing from a Single/Multi-function Device over a Traditional Telephone Line

A dispatcher from county A runs a NCIC query on an individual. The results are printed and then sent to an adjoining county using a single/multi-function device with facsimile capability. For faxing, the device is only connected to a traditional telephone line as is the device at the receiving county. Encryption of a document containing CJI is not required because the document travels over a traditional telephone line.

Use Case 3 – Faxing from a Multi-function Device over a Network

A dispatcher from city A runs a NCIC query on an individual. The results are printed and the dispatcher uses a multi-function copier to fax the file to a city in another state. The dispatcher enters the fax number of the receiver and sends the document. The document containing CJI is automatically converted to a digital file and routed to the receiver over the agency network and the Internet. Because the device uses a network and the Internet for transmitting documents containing CJI, encryption in transit using FIPS 140-2 certified 128 bit symmetric encryption is required.

5.11 Policy Area 11: Formal Audits

Formal audits are conducted to ensure compliance with applicable statutes, regulations and policies.

5.11.1 Audits by the FBI CJIS Division

5.11.1.1 Triennial Compliance Audits by the FBI CJIS Division

The FBI CJIS Division is authorized to conduct audits, once every three (3) years as a minimum, to assess agency compliance with applicable statutes, regulations and policies. The CJIS Audit Unit (CAU) shall conduct a triennial audit of each CSA in order to verify compliance with applicable statutes, regulations and policies. This audit shall include a sample of CJAs and, in coordination with the SIB, the NCJAs. Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies. The FBI CJIS Division shall also have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

5.11.1.2 Triennial Security Audits by the FBI CJIS Division

The FBI CJIS Division is authorized to conduct security audits of the CSA and SIB networks and systems, once every three (3) years as a minimum, to assess agency compliance with the CJIS Security Policy. This audit shall include a sample of CJAs and NCJAs. Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with the CJIS Security Policy.

5.11.2 Audits by the CSA

Each CSA shall:

1. At a minimum, triennially audit all CJAs and NCJAs which have direct access to the state system in order to ensure compliance with applicable statutes, regulations and policies.
2. In coordination with the SIB, establish a process to periodically audit all NCJAs, with access to CJL, in order to ensure compliance with applicable statutes, regulations and policies.
3. Have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.
4. Have the authority, on behalf of another CSA, to conduct a CSP compliance audit of contractor facilities and provide the results to the requesting CSA. If a subsequent CSA requests an audit of the same contractor facility, the CSA may provide the results of the previous audit unless otherwise notified by the requesting CSA that a new audit be performed.

Note: This authority does not apply to the audit requirement outlined in the Security and Management Control Outsourcing Standard for Non-Channeler and Channelers related to outsourcing noncriminal justice administrative functions.

5.11.3 Special Security Inquiries and Audits

All agencies having access to CJIS shall permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team shall be appointed by the APB and shall include at least one representative of the CJIS Division. All results of the inquiry and audit shall be reported to the APB with appropriate recommendations.

5.11.4 Compliance Subcommittees

The Criminal Justice Information Services (CJIS) Advisory Policy Board (APB) established the Compliance Evaluation Subcommittee (CES) to evaluate the results of audits conducted by the CJIS Audit Unit (CAU). The CES makes specific recommendations to the APB concerning compliance with applicable policies and regulations. The most current information regarding the CAU audits that are within the purview of the CES and detailed CES sanctions process procedures are available at CJIS.gov (Law Enforcement Enterprise Portal) CJIS Special Interest Groups CES Section and CJIS Section of FBI.gov.

The National Crime Prevention and Privacy Compact (Compact) Council at Article VI established the Compact Council (Council). The Compact Council Sanctions Committee is responsible for ensuring the use of the Interstate Identification Index System for noncriminal justice purposes complies with the Compact and with rules, standards, and procedures established by the Compact Council. As such, the Sanctions Committee reviews the results of audits conducted by the Federal Bureau of Investigation (FBI) of participants in the FBI's Criminal Justice Services (CJIS) Division programs. The Sanctions Committee reviews the audit results and the participant's response to determine a course of action necessary to bring the participant into compliance and make recommendations to the Compact Council or the FBI. Additional information on the Compact Council Sanctions process is available on the Compact Council's web-site.

Figure 15 – The Audit of a Local Police Department

A local police department implemented a replacement CAD system that integrated to their state's CSA and was authorized to process CJIS. Shortly after the implementation, their state's CSA conducted an audit of their policies, procedures, and systems that process CJIS. The police department supplied all architectural and policy documentation, including detailed network diagrams, to the auditors in order to assist them in the evaluation. The auditors discovered a deficiency in the police department's systems and marked them "out" in this aspect of the FBI CJIS Security Policy. The police department quickly addressed the deficiency and took corrective action, notifying the auditors of their actions.

5.12 Policy Area 12: Personnel Security

Having proper security measures against the insider threat is a critical component for the CJIS Security Policy. This section's security terms and requirements apply to all personnel who have unescorted access to unencrypted CJI including those individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

5.12.1 Personnel Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJI

1. To verify identification, state of residency and national fingerprint-based record checks shall be conducted prior to granting access to CJI for all personnel who have unescorted access to unencrypted CJI or unescorted access to physically secure locations or controlled areas (during times of CJI processing). However, if the person resides in a different state than that of the assigned agency, the agency shall conduct state (of the agency) and national fingerprint-based record checks and execute a NLETS CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances. When appropriate, the screening shall be consistent with:
 - a. 5 CFR 731.106; and/or
 - b. Office of Personnel Management policy, regulations, and guidance; and/or
 - c. agency policy, regulations, and guidance.

Federal entities bypassing state repositories in compliance with federal law may not be required to conduct a state fingerprint-based record check.

See Appendix J for applicable guidance regarding noncriminal justice agencies performing adjudication of civil fingerprint submissions.

2. All requests for access shall be made as specified by the CSO. The CSO, or their designee, is authorized to approve access to CJI. All CSO designees shall be from an authorized criminal justice agency.
3. If a record of any kind exists, access to CJI shall not be granted until the CSO or his/her designee reviews the matter to determine if access is appropriate.
 - a. If a felony conviction of any kind exists, the Interface Agency shall deny access to CJI. However, the Interface Agency may ask for a review by the CSO in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.
 - b. Applicants with a record of misdemeanor offense(s) may be granted access if the CSO, or his or her designee, determines the nature or severity of the misdemeanor offense(s) do not warrant disqualification. The Interface Agency may request the CSO review a denial of access determination. This same procedure applies if the person is found to be a fugitive or has an arrest history without conviction.
 - c. If a record of any kind is found on a contractor, the CGA shall be formally notified and system access shall be delayed pending review of the criminal history record information. The CGA shall in turn notify the contractor's security officer.

4. If the person appears to be a fugitive or has an arrest history without conviction, the CSO or his/her designee shall review the matter to determine if access to CJI is appropriate.
5. If the person already has access to CJI and is subsequently arrested and or convicted, continued access to CJI shall be determined by the CSO. This does not implicitly grant hiring/firing authority with the CSA, only the authority to grant access to CJI. For offenses other than felonies, the CSO has the latitude to delegate continued access determinations to his or her designee.
6. If the CSO or his/her designee determines that access to CJI by the person would not be in the public interest, access shall be denied and the person's appointing authority shall be notified in writing of the access denial.
7. The granting agency shall maintain a list of personnel who have been authorized unescorted access to unencrypted CJI and shall, upon request, provide a current copy of the access list to the CSO.

It is recommended individual background re-investigations be conducted every five years unless Rap Back is implemented.

5.12.2 Personnel Termination

Upon termination of personnel by an interface agency, the agency shall immediately terminate access to local agency systems with access to CJI. Furthermore, the interface agency shall provide notification or other action to ensure access to state and other agency systems is terminated. If the employee is an employee of a NCJA or a Contractor, the employer shall notify all Interface Agencies that may be affected by the personnel change.

5.12.3 Personnel Transfer

The agency shall review CJI access authorizations when personnel are reassigned or transferred to other positions within the agency and initiate appropriate actions such as closing and establishing accounts and changing system access authorizations.

5.12.4 Personnel Sanctions

The agency shall employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

Figure 16 – A Local Police Department's Personnel Security Controls

A local police department implemented a replacement CAD system that integrated to their state's CSA and was authorized to process CJI. In addition to the physical and technical controls already in place, the police department implemented a variety of personnel security controls to reduce the insider threat. The police department used background screening consistent with the FBI CJIS Security Policy to vet those with unescorted access to areas in which CJI is processed, including the IT administrators employed by a contractor and all janitorial staff. The police department established sanctions against any vetted person found to be in violation of stated

policies. The police department re-evaluated each person's suitability for access to CJI every five years.

5.13 Policy Area 13: Mobile Devices

This policy area describes considerations and requirements for mobile devices including smartphones and tablets. Mobile devices are not limited to a single form factor or communications medium. The requirements in this section augment those in other areas of the Policy to address the gaps introduced by using mobile devices.

The agency shall: (i) establish usage restrictions and implementation guidance for mobile devices; and (ii) authorize, monitor, control wireless access to the information system. Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections—without requiring network or peripheral cabling.

Appendix G provides reference material and additional information on mobile devices.

5.13.1 Wireless Communications Technologies

Examples of wireless communication technologies include, but are not limited to: 802.11, cellular, Bluetooth, satellite, microwave, and land mobile radio (LMR). Wireless technologies require at least the minimum security applied to wired technology and, based upon the specific technology or implementation, wireless technologies may require additional security controls as described below.

5.13.1.1 802.11 Wireless Protocols

Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) cryptographic algorithms, used by all pre-802.11i protocols, do not meet the requirements for FIPS 140-2 and shall not be used.

Agencies shall implement the following controls for all agency-managed wireless access points with access to an agency's network that processes unencrypted CJI:

1. Perform validation testing to ensure rogue APs (Access Points) do not exist in the 802.11 Wireless Local Area Network (WLAN) and to fully understand the wireless network security posture.
2. Maintain a complete inventory of all Access Points (APs) and 802.11 wireless devices.
3. Place APs in secured areas to prevent unauthorized physical access and user manipulation.
4. Test AP range boundaries to determine the precise extent of the wireless coverage and design the AP wireless coverage to limit the coverage area to only what is needed for operational purposes.
5. Enable user authentication and encryption mechanisms for the management interface of the AP.
6. Ensure that all APs have strong administrative passwords and ensure that all passwords are changed in accordance with Section 5.6.2.1.
7. Ensure the reset function on APs is used only when needed and is only invoked by authorized personnel. Restore the APs to the latest security settings, when the reset functions are used, to ensure the factory default settings are not utilized.

8. Change the default service set identifier (SSID) in the APs. Disable the broadcast SSID feature so that the client SSID must match that of the AP. Validate that the SSID character string does not contain any agency identifiable information (division, department, street, etc.) or services.
9. Enable all security features of the wireless product, including the cryptographic authentication, firewall, and other available privacy features.
10. Ensure that encryption key sizes are at least 128-bits and the default shared keys are replaced by unique keys.
11. Ensure that the ad hoc mode has been disabled.
12. Disable all nonessential management protocols on the APs.
13. Ensure all management access and authentication occurs via FIPS compliant secure protocols (e.g. SFTP, HTTPS, SNMP over TLS, etc.). Disable non-FIPS compliant secure access to the management interface.
14. Enable logging (if supported) and review the logs on a recurring basis per local policy. At a minimum logs shall be reviewed monthly.
15. Insulate, virtually (e.g. virtual local area network (VLAN) and ACLs) or physically (e.g. firewalls), the wireless network from the operational wired infrastructure. Limit access between wireless networks and the wired network to only operational needs.
16. When disposing of access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.

5.13.1.2 Cellular Devices

Cellular telephones, smartphones (i.e. Blackberry, iPhones, etc.), tablets, personal digital assistants (PDA), and “aircards” are examples of cellular handheld devices or devices that are capable of employing cellular technology. Additionally, cellular handheld devices typically include Bluetooth, infrared, and other wireless protocols capable of joining infrastructure networks or creating dynamic ad hoc networks.

Threats to cellular handheld devices stem mainly from their size, portability, and available wireless interfaces and associated services. Examples of threats to cellular handheld devices include:

1. Loss, theft, or disposal.
2. Unauthorized access.
3. Malware.
4. Spam.
5. Electronic eavesdropping.
6. Electronic tracking (threat to security of data and safety of the criminal justice professional).
7. Cloning (not as prevalent with later generation cellular technologies).
8. Server-resident data.

5.13.1.2.1 Cellular Service Abroad

Certain internal functions on cellular devices may be modified or compromised by the cellular carrier during international use as the devices are intended to have certain parameters configured by the cellular provider which is considered a “trusted” entity by the device.

When devices are authorized to access CJI outside the U.S., agencies shall perform an inspection to ensure that all controls are in place and functioning properly in accordance with the agency’s policies prior to and after deployment outside of the U.S.

5.13.1.2.2 Voice Transmissions Over Cellular Devices

Any cellular device used to transmit CJI via voice is exempt from the encryption and authentication requirements.

5.13.1.3 Bluetooth

Bluetooth is an open standard for short-range radio frequency (RF) communication. Bluetooth is used primarily to establish wireless personal area networks (WPAN). Bluetooth technology has been integrated into many types of business and consumer devices, including cell phones, laptops, automobiles, medical devices, printers, keyboards, mice, headsets, and biometric capture devices.

Bluetooth technology and associated devices are susceptible to general wireless networking threats (e.g. denial of service [DoS] attacks, eavesdropping, man-in-the-middle [MITM] attacks, message modification, and resource misappropriation) as well as specific Bluetooth-related attacks that target known vulnerabilities in Bluetooth implementations and specifications. Organizational security policy shall be used to dictate the use of Bluetooth and its associated devices based on the agency’s operational and business processes.

5.13.1.4 Mobile Hotspots

Many mobile devices include the capability to function as a WiFi hotspot that allows other devices to connect through the device to the internet over the devices cellular network.

When an agency allows mobile devices that are approved to access or store CJI to function as a Wi-Fi hotspot connecting to the Internet, they shall be configured:

1. Enable encryption on the hotspot
2. Change the hotspot’s default SSID
 - a. Ensure the hotspot SSID does not identify the device make/model or agency ownership
3. Create a wireless network password (Pre-shared key)
4. Enable the hotspot’s port filtering/blocking features if present
5. Only allow connections from agency controlled devices

Note: Refer to the requirements in Section 5.10.1.2 encryption for item #1. Refer to the requirements in Section 5.6.2.2.1 Password for item #3. Only password attributes #1, #2 and #3 are required.

OR

1. Have a MDM solution to provide the same security as identified in items 1 – 5 above.

5.13.2 Mobile Device Management (MDM)

Mobile Device Management (MDM) facilitates the implementation of sound security controls for mobile devices and allows for centralized oversight of configuration control, application usage, and device protection and recovery, if so desired by the agency.

Due to the potential for inconsistent network access or monitoring capability on mobile devices, methods used to monitor and manage the configuration of full featured operating systems may not function properly on devices with limited feature operating systems. MDM systems and applications coupled with device specific technical policy can provide a robust method for device configuration management if properly implemented.

Devices that have had any unauthorized changes made to them (including but not limited to being rooted or jailbroken) shall not be used to process, store, or transmit CJI data at any time. Agencies shall implement the following controls when allowing CJI access from devices running a limited-feature operating system:

1. Ensure that CJI is only transferred between CJI authorized applications and storage areas of the device.
2. MDM with centralized administration configured and implemented to perform at least the following controls:
 - a. Remote locking of device
 - b. Remote wiping of device
 - c. Setting and locking device configuration
 - d. Detection of “rooted” and “jailbroken” devices
 - e. Enforcement of folder or disk level encryption
 - f. Application of mandatory policy settings on the device
 - g. Detection of unauthorized configurations
 - h. Detection of unauthorized software or applications
 - i. Ability to determine the location of agency controlled devices
 - j. Prevention of unpatched devices from accessing CJI or CJI systems
 - k. Automatic device wiping after a specified number of failed access attempts

EXCEPTION: An MDM is not required when receiving CJI from an indirect access information system (i.e. the system provides no capability to conduct transactional activities on state and national repositories, applications or services). However, it is incumbent upon the authorized agency to ensure CJI is delivered to the appropriate requesting agency or individual. The CSO will make the final determination of whether access is considered indirect.

5.13.3 Wireless Device Risk Mitigations

Organizations shall, at a minimum, ensure that wireless devices:

1. Apply available critical patches and upgrades to the operating system as soon as they become available for the device and after necessary testing as described in Section 5.10.4.1.

2. Are configured for local device authentication (see Section 5.13.7.1).
3. Use advanced authentication or CSO approved compensating controls as per Section 5.13.7.2.1.
4. Encrypt all CJI resident on the device.
5. Erase cached information, to include authenticators (see Section 5.6.2.1) in applications, when session is terminated.
6. Employ personal firewalls on full-featured operating system devices or run a Mobile Device Management (MDM) system that facilitates the ability to provide firewall services from the agency level.
7. Employ malicious code protection on full-featured operating system devices or run a MDM system that facilitates the ability to provide anti-malware services from the agency level.

5.13.4 System Integrity

Managing system integrity on limited function mobile operating systems may require methods and technologies significantly different from traditional full featured operating systems. In many cases, the requirements of Section 5.10 of the CJIS Security Policy cannot be met with a mobile device without the installation of a third party MDM, application, or supporting service infrastructure.

5.13.4.1 Patching/Updates

Based on the varying connection methods for mobile devices, an always on connection cannot be guaranteed for patching and updating. Devices without always-on cellular connections may not be reachable for extended periods of time by the MDM or solution either to report status or initiate patching.

Agencies shall monitor mobile devices to ensure their patch and update state is current.

5.13.4.2 Malicious Code Protection

Appropriately configured MDM software is capable of checking the installed applications on the device and reporting the software inventory to a central management console in a manner analogous to traditional virus scan detection of unauthorized software and can provide a high degree of confidence that only known software or applications are installed on the device.

Agencies that allow smartphones and tablets to access CJI shall have a process to approve the use of specific software or applications on the devices. Any device natively capable of performing these functions without a MDM solution is acceptable under this section.

5.13.4.3 Personal Firewall

For the purpose of this policy, a personal firewall is an application that controls network traffic to and from a user device, permitting or denying communications based on policy. A personal firewall shall be employed on all mobile devices that have a full-feature operating system (i.e. laptops or tablets with Windows or Linux/Unix operating systems). At a minimum, the personal firewall shall perform the following activities:

1. Manage program access to the Internet.

2. Block unsolicited requests to connect to the user device.
3. Filter incoming traffic by IP address or protocol.
4. Filter incoming traffic by destination ports.
5. Maintain an IP traffic log.

Mobile devices with limited feature operating systems (i.e. tablets, smartphones) may not support a personal firewall. However, these operating systems have a limited number of system services installed, carefully controlled network access, and to a certain extent, perform functions similar to a personal firewall on a device with a full feature operating system. Appropriately configured MDM software is capable of controlling which applications are allowed on the device.

5.13.5 Incident Response

In addition to the requirements in Section 5.3 Incident Response, agencies shall develop additional or enhanced incident reporting and handling procedures to address mobile device operating scenarios. Rapid response to mobile device related incidents can significantly mitigate the risks associated with illicit data access either on the device itself or within online data resources associated with the device through an application or specialized interface.

Special reporting procedures for mobile devices shall apply in any of the following situations:

1. Loss of device control. For example:
 - a. Device known to be locked, minimal duration of loss
 - b. Device lock state unknown, minimal duration of loss
 - c. Device lock state unknown, extended duration of loss
 - d. Device known to be unlocked, more than momentary duration of loss
2. Total loss of device
3. Device compromise
4. Device loss or compromise outside the United States

5.13.6 Access Control

Multiple user accounts are not generally supported on limited feature mobile operating systems. Access control (Section 5.5 Access Control) shall be accomplished by the application that accesses CJI.

5.13.7 Identification and Authentication

Due to the technical methods used for identification and authentication on many limited feature mobile operating systems, achieving compliance may require many different components.

5.13.7.1 Local Device Authentication

When mobile devices are authorized for use in accessing CJI, local device authentication shall be used to unlock the device for use. The authenticator used shall meet the requirements in section 5.6.2.1 Standard Authenticators.

5.13.7.2 Advanced Authentication

When accessing CJI from an authorized mobile device, advanced authentication shall be used by the authorized user unless the access to CJI is indirect as described in Section 5.6.2.2.1. If access is indirect, then AA is not required.

5.13.7.2.1 Compensating Controls

CSO approved compensating controls to meet the AA requirement on agency-issued smartphones and tablets with limited feature operating systems are permitted. Compensating controls are temporary control measures that are implemented in lieu of the required AA control measures when an agency cannot meet a requirement due to legitimate technical or business constraints. Before CSOs consider approval of compensating controls, Mobile Device Management (MDM) shall be implemented per Section 5.13.2. The compensating controls shall:

1. Meet the intent of the CJIS Security Policy AA requirement
2. Provide a similar level of protection or security as the original AA requirement
3. Not rely upon the existing requirements for AA as compensating controls
4. Expire upon the CSO approved date or when a compliant AA solution is implemented.

Additionally, compensating controls may rely upon other, non-AA, existing requirements as compensating controls and/or be combined with new controls to create compensating controls.

The compensating controls for AA are a combination of controls providing acceptable assurance only the authorized user is authenticating and not an impersonator or (in the case of agency-issued device used by multiple users) controls that reduce the risk of exposure if information is accessed by an unauthorized party.

The following minimum controls shall be implemented as part of the CSO approved compensating controls:

- Possession and registration of an agency issued smartphone or tablet as an indication it is the authorized user
- Use of device certificates per Section 5.13.7.3 Device Certificates
- Implemented CJIS Security Policy compliant standard authenticator protection on the secure location where CJI is stored

5.13.7.3 Device Certificates

Device certificates are often used to uniquely identify mobile devices using part of a public key pair on the device in the form of a public key certificate. While there is value to ensuring the device itself can authenticate to a system supplying CJI, and may provide a critical layer of device identification or authentication in a larger scheme, a device certificate alone placed on the device shall not be considered valid proof that the device is being operated by an authorized user.

When certificates or cryptographic keys used to authenticate a mobile device are used in lieu of compensating controls for advanced authentication, they shall be:

1. Protected against being extracted from the device
2. Configured for remote wipe on demand or self-deletion based on a number of unsuccessful login or access attempts
3. Configured to use a secure authenticator (i.e. password, PIN) to unlock the key for use

APPENDICES

APPENDIX A TERMS AND DEFINITIONS

Access to Criminal Justice Information — The physical or logical (electronic) ability, right or privilege to view, modify or make use of Criminal Justice Information.

Administration of Criminal Justice — The detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. It also includes criminal identification activities; the collection, storage, and dissemination of criminal history record information; and criminal justice employment. In addition, administration of criminal justice includes “crime prevention programs” to the extent access to criminal history record information is limited to law enforcement agencies for law enforcement programs (e.g. record checks of individuals who participate in Neighborhood Watch or “safe house” programs) and the result of such checks will not be disseminated outside the law enforcement agency.

Agency Controlled Mobile Device — A mobile device that is centrally managed by an agency for the purpose of securing the device for potential access to CJI. The device can be agency issued or BYOD (personally owned).

Agency Coordinator (AC) — A staff member of the Contracting Government Agency who manages the agreement between the Contractor and agency.

Agency Issued Mobile Device — A mobile device that is owned by an agency and issued to an individual for use. It is centrally managed by the agency for the purpose of securing the device for potential access to CJI. The device is not BYOD (personally owned).

Agency Liaison (AL) — Coordinator of activities between the criminal justice agency and the noncriminal justice agency when responsibility for a criminal justice system has been delegated by a criminal justice agency to a noncriminal justice agency, which has in turn entered into an agreement with a contractor. The agency liaison shall, inter alia, monitor compliance with system security requirements. In instances in which the noncriminal justice agency's authority is directly from the CJIS systems agency, there is no requirement for the appointment of an agency liaison.

Asymmetric Encryption — A type of encryption that uses key pairs for encryption. One key is used to encrypt a message and another key to decrypt the message. Asymmetric encryption is also commonly known as public key encryption.

Authorized User/Personnel — An individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI.

Authorized Recipient — (1) A criminal justice agency or federal agency authorized to receive CHRI pursuant to federal statute or executive order; (2) A nongovernmental entity authorized by federal statute or executive order to receive CHRI for noncriminal justice purposes; or (3) A government agency authorized by federal statute or executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.

Availability — The degree to which information, a system, subsystem, or equipment is operable and in a useable state; frequently represented as a proportion of time the element is in a functioning condition.

Biographic Data — Information collected about individuals associated with a unique case, and not necessarily connected to identity data. Biographic Data does not provide a history of an individual, only information related to a unique case.

Biometric Data — When applied to CJL, it is used to identify individuals, and includes the following types: fingerprints, palm prints, DNA, iris, and facial recognition.

Case / Incident History — All relevant information gathered about an individual, organization, incident, or combination thereof, arranged so as to serve as an organized record to provide analytic value for a criminal justice organization. In regards to CJL, it is the information about the history of criminal incidents.

Certificate Authority (CA) Certificate — Digital certificates required for certificate-based authentication that are issued to tell the client computers and servers that it can trust other certificates that are issued by this CA.

Channeler — A FBI approved contractor, who has entered into an agreement with an Authorized Recipient(s), to receive noncriminal justice applicant fingerprint submissions and collect the associated fees. The Channeler ensures fingerprint submissions are properly and adequately completed, electronically forwards fingerprint submissions to the FBI's CJIS Division for national noncriminal justice criminal history record check, and receives electronic record check results for dissemination to Authorized Recipients. A Channeler is essentially an "expediter" rather than a user of criminal history record check results.

Cloud Client — A machine or software application that accesses cloud services over a network connection, perhaps on behalf of a subscriber.

Cloud Computing — A distributed computing model that permits on-demand network access to a shared pool of configurable computing resources (i.e., networks, servers, storage, applications, and services), software, and information.

Cloud Provider — An organization that provides cloud computing services.

Cloud Subscriber — A person or organization that is a customer of a cloud computing service provider.

CJIS Advisory Policy Board (APB) — The governing organization within the FBI CJIS Advisory Process composed of representatives from criminal justice and national security agencies within the United States. The APB reviews policy, technical, and operational issues relative to CJIS Division programs and makes subsequent recommendations to the Director of the FBI.

CJIS Audit Unit (CAU) — The organization within the FBI CJIS Division responsible to perform audits of CSAs to verify compliance with the CJIS Security Policy.

CJIS Security Policy — The FBI CJIS Security Policy document as published by the FBI CJIS ISO; the document containing this glossary.

CJIS Systems Agency (CSA) — A duly authorized state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users with respect to the CJL from various systems managed by the FBI CJIS

Division. There shall be only one CSA per state or territory. In federal agencies, the CSA may be the interface or switch to other federal agencies connecting to the FBI CJIS systems.

CJIS Systems Agency Information Security Officer (CSA ISO) — The appointed FBI CJIS Division personnel responsible to coordinate information security efforts at all CJIS interface agencies.

CJIS Systems Officer (CSO) — The individual located within the CJIS Systems Agency responsible for the administration of the CJIS network on behalf of the CJIS Systems Agency.

Compact Council — The entity created by the National Crime Prevention and Privacy Compact of 1998 that has the authority to promulgate rules and procedures governing the use of the III system for noncriminal justice purposes.

Compact Officers — The leadership of the Compact Council, oversees the infrastructure established by the National Crime Prevention and Privacy Compact Act of 1998, which is used by ratifying states to exchange criminal records for noncriminal justice purposes. Their primary responsibilities are to promulgate rules and procedures for the effective and appropriate use of the III system.

Compensating Controls — Compensating controls are temporary control measures implemented in lieu of the required control measures when an agency cannot meet the AA requirement due to legitimate technical or business constraints. The compensating controls must:

1. Meet the intent of the CJIS Security Policy AA requirement
2. Provide a similar level of protection or security as the original AA requirement
3. Not rely upon the existing requirements for AA as compensating controls

Additionally, compensating controls may rely upon other, non-AA, existing requirements as compensating controls and/or be combined with new controls to create compensating controls.

Computer Security Incident Response Capability (CSIRC) — A collection of personnel, systems, and processes that are used to efficiently and quickly manage a centralized response to any sort of computer security incident which may occur.

Confidentiality — The concept of ensuring that information is observable only to those who have been granted authorization to do so.

Contractor — A private business, agency or individual which has entered into an agreement for the administration of criminal justice or noncriminal justice functions with a Criminal Justice Agency or a Noncriminal Justice Agency. Also, a private business approved by the FBI CJIS Division to contract with Noncriminal Justice Agencies to perform noncriminal justice functions associated with civil fingerprint submission for hiring purposes.

Contracting Government Agency (CGA) — The government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor.

Crime Reports Data — The data collected through the Uniform Crime Reporting program and reported upon annually by the FBI CJIS division used to analyze the crime statistics for the United States.

Criminal History Record Information (CHRI) — A subset of CJI. Any notations or other written or electronic evidence of an arrest, detention, complaint, indictment, information or other formal criminal charge relating to an identifiable person that includes identifying information regarding the individual as well as the disposition of any charges.

Criminal Justice Agency (CJA) — The courts, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

Criminal Justice Agency User Agreement — A terms-of-service agreement that must be signed prior to accessing CJI. This agreement is required by each CJA and spells out user's responsibilities, the forms and methods of acceptable use, penalties for their violation, disclaimers, and so on.

Criminal Justice Conveyance — A criminal justice conveyance is any enclosed mobile vehicle used for the purposes of criminal justice activities with the capability to comply, during operational periods, with the requirements of Section 5.9.1.3.

Criminal Justice Information (CJI) — Criminal Justice Information is the abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions. The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g. ORI, NIC, UCN, etc.) when not accompanied by information that reveals CJI or PII.

Criminal Justice Information Services Division (FBI CJIS or CJIS) — The FBI division responsible for the collection, warehousing, and timely dissemination of relevant CJI to the FBI and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

Data — See Information and CJI.

Decryption — The inverse cryptographic operation used to convert encrypted information back into a plaintext (readable) format.

Degauss — Neutralize a magnetic field to erase information from a magnetic disk or other storage device. In the field of information technology, degauss has become synonymous with erasing information whether or not the medium is magnetic. In the event the device to be degaussed is not magnetic (e.g. solid state drive, USB storage device), steps other than magnetic degaussing may be required to render the information irretrievable from the device.

Department of Justice (DoJ) — The Department within the U.S. Government responsible to enforce the law and defend the interests of the United States according to the law, to ensure public safety against threats foreign and domestic, to provide federal leadership in preventing and controlling crime, to seek just punishment for those guilty of unlawful behavior, and to ensure fair and impartial administration of justice for all Americans.

Digital Media – Any form of electronic media designed to store data in a digital format. This includes, but is not limited to: memory device in laptops, computers, and mobile devices; and any removable, transportable electronic media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card.

Digital Signature – A digital signature consists of three algorithms: (1) A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key. (2) A signing algorithm that, given a message and a private key, produces a signature. (3) A signature verifying algorithm that, given a message, public key, and a signature, either accepts or rejects the message's claim to authenticity. Two main properties are required. First, a signature generated from a fixed message and fixed private key should verify the authenticity of that message by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party who does not possess the private key.

Direct Access — (1) Having the authority to access systems managed by the FBI CJIS Division, whether by manual or automated methods, not requiring the assistance of, or intervention by, any other party or agency (28 CFR, Chapter 1, Part 20). (2) Having the authority to query or update national databases maintained by the FBI CJIS Division including national queries and updates automatically or manually generated by the CSA.

Dissemination — The transmission/distribution of CJI to Authorized Recipients within an agency.

Encryption – A form of cryptology that applies a cryptographic operation to provide confidentiality of (sensitive) information.

Escort – Authorized personnel who accompany a visitor at all times while within a physically secure location to ensure the protection and integrity of the physically secure location and any Criminal Justice Information therein. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.

Facsimile (Fax) – Facsimile is: (a) a document received and printed on a single or multi-function stand-alone device, (b) a single or multi-function stand-alone device for the express purpose of transmitting and receiving documents from a like device over a standard telephone line, or (c) a facsimile server, application, service which implements email-like technology and transfers documents over a network.

Federal Bureau of Investigation (FBI) — The agency within the DOJ responsible to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners.

FBI CJIS Information Security Officer (FBI CJIS ISO) — The FBI personnel responsible for the maintenance and dissemination of the FBI CJIS Security Policy; the liaison between the FBI and the CSA's ISOs and other relevant security points-of-contact (POCs); the provider of technical guidance as to the intent and implementation of technical policy issues; the POC for computer incident notification which also disseminates security alerts to the CSOs and ISOs.

Federal Information Security Management Act (FISMA) — The Federal Information Security Management Act of 2002, a US Federal law that established information security standards for the protection of economic and national security interests of the United States. It requires each federal agency to develop, document, and implement an agency-wide program to provide information

security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

For Official Use Only (FOUO) — A caveat applied to unclassified sensitive information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA), 5 U.S.C 522. In general, information marked FOUO shall not be disclosed to anybody except Government (Federal, State, tribal, or local) employees or contractors with a need to know.

Full-feature Operating System — Full-feature operating systems are traditional operating systems used by a standard desktop computer (e.g. Microsoft Windows, Apple OSX/macOS, LINUX/UNIX, etc.). These operating systems are generally open to user control and configuration and therefore require configuration management to properly secure, or “harden”, these devices from malicious network based technical attacks (e.g. malware, spyware, hackers, etc.). These operating systems require traditional protection applications such as antivirus programs and personal firewalls.

Guest Operating System — An operating system that has emulated hardware presented to it by a host operating system. Also referred to as the virtual machine (VM).

Hash Value — The term that refers to an alphanumeric value which represents the result of applying a cryptographic hash function to data.

Hashing — The process of applying a mathematical algorithm to data to produce an alphanumeric value (i.e. hash value) to be used as a representative of that data.

Host Operating System — In the context of virtualization, the operating system that interfaces with the actual physical hardware and arbitrates between it and the guest operating systems. It is also referred to as a hypervisor.

Hybrid Encryption — A type of encryption where both asymmetric encryption and symmetric encryption keys are used creating what is referred to as cipher suites. In a hybrid solution the asymmetric encryption keys are used for client/server certificate exchange to provide session integrity while the symmetric encryption keys are used for bulk data encryption to provide data confidentiality.

Hypervisor — See Host Operating System.

Identity History Data — Textual data that corresponds with an individual’s biometric data, providing a history of criminal and/or civil events for the identified individual.

In-Band – The communication service channel (network connection, email, SMS text, phone call, etc.) used to obtain an authenticator is the same as the one used for login.

Indirect Access – Having the authority to access systems containing CJI without providing the user the ability to conduct transactional activities (the capability to query or update) on state and national systems (e.g. CJIS Systems Agency (CSA), State Identification Bureau (SIB), or national repositories).

Information — See data and CJI.

Information Exchange Agreement — An agreement that codifies the rules by which two parties engage in the sharing of information. These agreements typically include language which establishes some general duty-of-care over the other party’s information, whether and how it can be further disseminated, penalties for violations, the laws governing the agreement (which

establishes venue), procedures for the handling of shared information at the termination of the agreement, and so on. This document will ensure consistency with applicable federal laws, directives, policies, regulations, standards and guidance.

Information Security Officer (ISO) — Typically a member of an organization who has the responsibility to establish and maintain information security policy, assesses threats and vulnerabilities, performs risk and control assessments, oversees the governance of security operations, and establishes information security training and awareness programs. The ISO also usually interfaces with security operations to manage implementation details and with auditors to verify compliance to established policies.

Information System — A system of people, data, and processes, whether manual or automated, established for the purpose of managing information.

Integrated Automated Fingerprint Identification System (IAFIS) — The national fingerprint and criminal history system maintained by the FBI CJIS Division that provides the law enforcement community with automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses.

Integrity — The perceived consistency of expected outcomes, actions, values, and methods of an individual or organization. As it relates to data, it is the concept that data is preserved in a consistent and correct state for its intended use.

Interconnection Security Agreement (ISA) — An agreement much like an Information Exchange Agreement as mentioned above, but concentrating more on formalizing the technical and security requirements pertaining to some sort of interface between the parties' information systems.

Interface Agency — A legacy term used to describe agencies with direct connections to the CSA. This term is now used predominantly in a common way to describe any sub-agency of a CSA or SIB that leverages the CSA or SIB as a conduit to FBI CJIS information.

Internet Protocol (IP) — A protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses.

Interstate Identification Index (III) — The CJIS service that manages automated submission and requests for CHRI that is warehoused subsequent to the submission of fingerprint information. Subsequent requests are directed to the originating State as needed.

Intrusion Detection — The process of monitoring the events occurring in an information system or network and analyzing them for signs of possible incidents.

Intrusion Detection System — Software which automates the intrusion detection process.

Intrusion Prevention — The process of monitoring events occurring in an information system or network and analyzing them for signs of possible incidents and attempting to stop detected possible incidents.

Intrusion Prevention System — Software which has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents.

Jailbreak (Jailbroken) — The process of attaining privileged control (known as “root access”) of a device running the Apple iOS operating system that ultimately allows a user the ability to alter or replace system applications and settings, run specialized applications that require administrator-level permissions, or perform other operations that are otherwise not allowed.

Laptop Devices – Laptop devices are mobile devices with a full-featured operating system (e.g. Microsoft Windows, Apple OSX/macOS, LINUX/UNIX, etc.). Laptops are typically intended for transport via vehicle mount or portfolio-sized carry case, but not on the body. This definition does not include pocket/handheld devices (e.g. smartphones), or mobile devices that feature a limited feature operating system (e.g. tablets).

Law Enforcement Enterprise Portal (LEEP) — A secure, Internet-based communications portal provided by the FBI CJIS Division for use by law enforcement, first responders, criminal justice professionals, and anti-terrorism and intelligence agencies around the globe. Its primary purpose is to provide a platform on which various law enforcement agencies can collaborate on FOUO matters.

Limited-feature Operating System — Limited-feature operating systems are designed specifically for the mobile environment where battery life and power efficiency are primary design drivers (e.g. Apple iOS, Android, Windows Mobile, Blackberry OS, etc.). These operating systems permit limited user control, but are inherently more resistant than a full-feature operating system to certain types of network based technical attacks due to the limited feature sets. Devices using these operating systems are required to be managed by a mobile device management solution.

Logical Access – The technical means (e.g., read, create, modify, delete a file, execute a program, or use an external connection) for an individual or other computer system to utilize CJI or CJIS applications.

Logical Partitioning – When the host operating system, or hypervisor, allows multiple guest operating systems to share the same physical resources.

Local Agency Security Officer (LASO) — The primary Information Security contact between a local law enforcement agency and the CSA under which this agency interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to Information Security, disseminates Information Security alerts and other material to their constituents, maintains Information Security documentation (including system configuration data), assists with Information Security audits of hardware and procedures, and keeps the CSA informed as to any Information Security needs and problems.

Management Control Agreement (MCA) — An agreement between parties that wish to share or pool resources that codifies precisely who has administrative control over, versus overall management and legal responsibility for, assets covered under the agreement. An MCA must ensure the CJA’s authority remains with regard to all aspects of Section 3.2.2. The MCA usually results in the CJA having ultimate authority over the CJI supporting infrastructure administered by the NCJA.

Metadata — Structured information that describes, explains, locates or otherwise makes it easier to retrieve, use or manage an information resource. Metadata is commonly referred to as data about data, information about information, or information describing the characteristics of data.

Mobile Device — Any portable device used to access CJI via a wireless connection (e.g. cellular, WiFi, Bluetooth, etc.).

Mobile Device Management (MDM) — Centralized administration and control of mobile devices specifically including, but not limited to, cellular phones, smart phones, and tablets. Management typically includes the ability to configure device settings and prevent a user from changing them, remotely locating a device in the event of theft or loss, and remotely locking or wiping a device. Management can also include over-the-air distribution of applications and updating installed applications.

Mobile (WiFi) Hotspot — A mobile (WiFi) hotspot is a zone or area associated with a mobile device (e.g. smartphone, air card) allowing wireless connectivity to the Internet typically through a cellular connection.

National Crime Information Center (NCIC) — An information system which stores CJI which can be queried by appropriate Federal, state, and local law enforcement and other criminal justice agencies.

National Instant Criminal Background Check System (NICS) — A system mandated by the Brady Handgun Violence Prevention Act of 1993 that is used by Federal Firearms Licensees (FFLs) to instantly determine via telephone or other electronic means whether the transfer of a firearm would be in violation of Section 922 (g) or (n) of Title 18, United States Code, or state law, by evaluating the prospective buyer's criminal history.

National Institute of Standards and Technology (NIST) — Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce whose mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic and national security.

Noncriminal Justice Agency (NCJA) — A governmental agency, or any subunit thereof, that provides services primarily for purposes other than the administration of criminal justice. Examples of services include, but not limited to, employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

NCJA (Government) — A Federal, state, local, or tribal governmental agency or any subunit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJI. An example would be the central IT organization within a state government that administers equipment on behalf of a state law-enforcement agency.

NCJA (Private) — A private agency or subunit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJI. An example would include a local bank.

NCJA (Public) — A public agency or sub-unit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJI. An example would include a county school board which uses CHRI to assist in employee hiring decisions.

Noncriminal Justice Purpose — The uses of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

Office of Management and Budget (OMB) — The agency within the Executive Branch of the Federal government responsible to oversee the preparation of the federal budget, to assist in the

supervision of other Executive Branch agencies, and to oversee and coordinate the Presidential Administration's procurement, financial management, information, and regulatory policies.

One-time Password — A disposable, single-use standard authenticator for access CJI. One-time passwords are: minimum of six (6) randomly generated characters, valid for a single session, and if not used, expire within a minimum of five (5) minutes after issuance.

Out-of-Band — The communication service channel (network connection, email, SMS text, phone call, etc.) used to obtain an authenticator is separate from that used for login.

Outsourcing — The process of delegating in-house operations to a third-party. For instance, when the administration of criminal justice functions (network operations, dispatch functions, system administration operations, etc.) are performed for the criminal justice agency by a city or county information technology department or are contracted to be performed by a vendor.

Outsourcing Standard — National Crime Prevention and Privacy Compact Council's Outsourcing Standard. The Compact Council's uniform standards and processes for the interstate and Federal-State exchange of criminal history records for noncriminal justice purposes.

Partitioning – Managing guest operating system, or virtual machine, access to hardware so that each guest OS can access its own resources but cannot encroach on the other guest operating systems resources or any resources not allocated for virtualization use.

Password Verifier (Verifier) – An entity or process that verifies the claimant's identity by verifying the claimant's possession and control of one or two authenticators using an authentication protocol. To do this, the Verifier may also need to validate credentials that link the authenticator(s) to the subscriber's identifier and check their status.

Personal Firewall — An application which controls network traffic to and from a computer, permitting or denying communications based on a security policy.

Personally Identifiable Information (PII) — PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

Physical Access – The physical ability, right or privilege to view, modify or make use of Criminal Justice Information (CJI) by means of physical presence within the proximity of computers and network devices (e.g. the ability to insert a boot disk or other device into the system, make a physical connection with electronic equipment, etc.).

Physical Media – Physical media refers to media in printed form. This definition includes, but is not limited to, printed documents, printed imagery, printed facsimile.

Physical Partitioning – When the host operating system, or hypervisor, assigns separate physical resources to each guest operating systems, or virtual machine.

Physically Secure Location — A facility, a criminal justice conveyance, or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems.

Pocket/Handheld Mobile Device – Pocket/Handheld mobile devices (e.g. smartphones) are intended to be carried in a pocket or holster attached to the body and feature an operating system

with limited functionality (e.g., iOS, Android, BlackBerry, etc.). This definition does not include tablet and laptop devices.

Property Data — Information about vehicles and property associated with a crime.

Rap Back — A NGI service that allows authorized agencies to receive notification of subsequent criminal activity reported to the FBI committed by persons of interest.

Receive-Only Terminal (ROT) – A device that is configured to accept a limited type of data but is technically prohibited from forming or transmitting data, browsing or navigating internal or external networks, or otherwise performing outside the scope of receive only (e.g., a printer, dumb terminal, etc.).

Repository Manager, or Chief Administrator — The designated manager of the agency having oversight responsibility for a CSA's fingerprint identification services. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the repository manager and CSO may be the same person.

Root (Rooting, Rooted) — The process of attaining privileged control (known as “root access”) of a device running the Android operating system that ultimately allows a user the ability to alter or replace system applications and settings, run specialized applications that require administrator-level permissions, or perform other operations that are otherwise not allowed.

Salting –The process of applying a non-secret value to data prior to applying a cryptographic process, such as hashing. This process changes the value to be hashed in a manner designed to ensure an attacker cannot reuse the results of computations for one instance.

Secondary Dissemination — The promulgation of CJI from a releasing agency to an authorized recipient agency when the recipient agency has not been previously identified in a formal information exchange agreement.

Security Addendum (SA) — A uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to criminal history record information, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information consistent with existing regulations and the CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require.

Sensitive But Unclassified (SBU) — Designation of information in the United States federal government that, though unclassified, often requires strict controls over its distribution. SBU is a broad category of information that includes material covered by such designations as For Official Use Only (FOUO), Law Enforcement Sensitive (LES), Sensitive Homeland Security Information, Security Sensitive Information (SSI), Critical Infrastructure Information (CII), etc. Some categories of SBU information have authority in statute or regulation (e.g. SSI, CII) while others, including FOUO, do not. As of May 9, 2008, the more appropriate terminology to use is Controlled Unclassified Information (CUI).

Server/Client Computer Certificate (device-based) – Digital certificates that are issued to servers or client computers or devices by a CA and used to prove device identity between server and/or client computer devices during the authentication process.

Service — The organized system of apparatus, appliances, personnel, etc., that supply some tangible benefit to the consumers of this service. In the context of CJIS, this usually refers to one of the applications that can be used to process CJIS.

Shredder — A device used for shredding documents, often as a security measure to prevent unapproved persons from reading them. Strip-cut shredders, also known as straight-cut or spaghetti-cut, slice the paper into long, thin strips but are not considered secure. Cross-cut shredders provide more security by cutting paper vertically and horizontally into confetti-like pieces.

Smartphone — See pocket/handheld mobile devices.

Social Engineering — The act of manipulating people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victim.

Software Patch — A piece of software designed to fix problems with, or update, a computer program or its supporting data. This includes fixing security vulnerabilities and other bugs and improving the usability or performance. Though meant to fix problems, poorly designed patches can sometimes introduce new problems. As such, patches should be installed in a test environment prior to being installed in a live, operational system. Patches often can be found in multiple locations but should be retrieved only from sources agreed upon through organizational policy.

State and Federal Agency User Agreement — A written agreement that each CSA or SIB Chief shall execute with the FBI CJIS Division stating their willingness to demonstrate conformance with the FBI CJIS Security Policy prior to the establishment of connectivity between organizations. This agreement includes the standards and sanctions governing use of CJIS systems, as well as verbiage to allow the FBI to periodically audit the CSA as well as to allow the FBI to penetration test its own network from the CSA's interfaces to it.

State Compact Officer — The representative of a state that is party to the National Crime Prevention and Privacy Compact, and is the chief administrator of the state's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.

State Identification Bureau (SIB) — The state agency with the responsibility for the state's fingerprint identification services.

State Identification Bureau (SIB) Chief — The SIB Chief is the designated manager of state's SIB. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the SIB Chief and CSO may be the same person.

State of Residency — A state of residency is the state in which an individual claims and can provide documented evidence as proof of being his/her permanent living domicile. CJIS Systems Officers have the latitude to determine what documentation constitutes acceptable proof of residency.

Symmetric Encryption — A type of encryption where the same key is used to encrypt and decrypt a message. Symmetric encryption is also known as secret key encryption.

System — Refer to connections to the FBI's criminal justice information repositories and the equipment used to establish said connections. In the context of CJIS, this usually refers to

applications and all interconnecting infrastructure required to use those applications that process CJI.

Tablet Devices – Tablet devices are mobile devices with a limited feature operating system (e.g. iOS, Android, Windows RT, etc.). Tablets typically consist of a touch screen without a permanently attached keyboard intended for transport via vehicle mount or portfolio-sized carry case but not on the body. This definition does not include pocket/handheld devices (e.g. smartphones) or mobile devices with full-featured operating systems (e.g. laptops).

Terminal Agency Coordinator (TAC) — Serves as the point-of-contact at the local agency for matters relating to CJIS information access. A TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with CJIS systems policies.

User Certificate (user-based) – Digital certificates that are unique and issued to individuals by a CA. Though not always required to do so, these specific certificates are often embedded on smart cards or other external devices as a means of distribution to specified users. This certificate is used when individuals need to prove their identity during the authentication process.

Virtual Escort – Authorized personnel who actively monitor a remote maintenance session on Criminal Justice Information (CJI)-processing systems. The escort must have the ability to end the session at any time deemed necessary to ensure the protection and integrity of CJI at all times.

Virtual Machine (VM) – See Guest Operating System

Virtualization — Refers to a methodology of dividing the resources of a computer (hardware and software) into multiple execution environments, by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing, partial or complete machine simulation or emulation allowing multiple operating systems, or images, to run concurrently on the same hardware.

Voice over Internet Protocol (VoIP) — A set of software, hardware, and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network, or across the Internet.

Wireless Access Point – A wireless access point is a device that logically connects a wireless client device to an organization's enterprise network which processes unencrypted CJI.

Wireless (WiFi) Hotspot – A wireless (WiFi) hotspot is a zone or area within a fixed location allowing wireless connectivity to the Internet typically through a wired connection. Hotspots are typically available in public areas such as airports, hotels and restaurants.

APPENDIX B ACRONYMS

Acronym	Term
AA	Advanced Authentication
AC	Agency Coordinator
ACL	Access Control List
AES	Advanced Encryption Standard
AP	Access Point
APB	Advisory Policy Board
BD-ADDR	Bluetooth-Enabled Wireless Devices and Addresses
BYOD	Bring Your Own Device
CAD	Computer-Assisted Dispatch
CAU	CJIS Audit Unit
CFR	Code of Federal Regulations
CGA	Contracting Government Agency
CHRI	Criminal History Record Information
CJA	Criminal Justice Agency
CJI	Criminal Justice Information
CJIS	Criminal Justice Information Services
ConOps	Concept of Operations
CSA	CJIS Systems Agency
CSIRC	Computer Security Incident Response Capability
CSO	CJIS Systems Officer
DAA	Designated Approving Authority
DoJ	Department of Justice

DoJCBERT	DoJ Computer Emergency Response Team
FBI	Federal Bureau of Investigation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FOUO	For Official Use Only
HIDS	Host-based Intrusion Detection System
HIPS	Host-based Intrusion Prevention System
HTTP	Hypertext Transfer Protocol
IAPIS	Integrated Automated Fingerprint Identification System
IDS	Intrusion Detection System
III	Interstate Identification Index
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSEC	Internet Protocol Security
ISA	Interconnection Security Agreement
ISO	Information Security Officer
IT	Information Technology
LASO	Local Agency Security Officer
LEEP	Law Enforcement Enterprise Portal
LMR	Land Mobile Radio
MAC	Media Access Control
MCA	Management Control Agreement
MDM	Mobile Device Management
MITM	Man-in-the-Middle

MOU	Memorandum of Understanding
NCIC	National Crime Information Center
NCJA	Noncriminal Justice Agency
NICS	National Instant Criminal Background Check System
NIDS	Network-based Intrusion Detection System
NIPS	Network-based Intrusion Prevention System
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
ORI	Originating Agency Identifier
OTP	One-time Password
PBX	Private Branch Exchange
PCSC	Preventing and Combating Serious Crime
PDA	Personal Digital Assistant
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POC	Point-of-Contact
PSTN	Public Switched Telephone Network
QA	Quality Assurance
QoS	Quality of Service
RCMP	Royal Canadian Mounted Police
RF	Radio Frequency
SA	Security Addendum
SCO	State Compact Officer
SIB	State Identification Bureau

SIG	Special Interest Group
SP	Special Publication
SPRC	Security Policy Resource Center
SSID	Service Set Identifier
TAC	Terminal Agency Coordinator
TLS	Transport Layer Security
UCN	Universal Control Number
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

APPENDIX C NETWORK TOPOLOGY DIAGRAMS

Network diagrams, i.e. topological drawings, are an essential part of solid network security. Through graphical illustration, a comprehensive network diagram provides the “big picture” – enabling network managers to quickly ascertain the interconnecting nodes of a network for a multitude of purposes, including troubleshooting and optimization. Network diagrams are integral to demonstrating the manner in which each agency ensures criminal justice data is afforded appropriate technical security protections and is protected during transit and at rest.

The following diagrams, labeled Appendix C.1-A through C.1-D, are examples for agencies to utilize during the development, maintenance, and update stages of their own network diagrams. By using these example drawings as a guideline, agencies can form the foundation for ensuring compliance with Section 5.7.1.2 of the CJIS Security Policy.

The purpose for including the following diagrams in this Policy is to aid agencies in their understanding of diagram expectations and should not be construed as a mandated method for network topologies. It should also be noted that agencies are not required to use the identical icons depicted in the example diagrams and should not construe any depiction of a particular vendor product as an endorsement of that product by the FBI CJIS Division.

Appendix C.1-A is a conceptual overview of the various types of agencies that can be involved in handling of CJL, and illustrates several ways in which these interconnections might occur. This diagram is not intended to demonstrate the level of detail required for any given agency’s documentation, but it provides the reader with some additional context through which to digest the following diagrams. Take particular note of the types of network interfaces in use between agencies, in some cases dedicated circuits with encryption mechanisms, and in other cases VPNs over the Internet. This diagram attempts to show the level of diversity possible within the law enforcement community. These diagrams in no way constitute a standard for network engineering, but rather, for the expected quality of documentation.

The next three topology diagrams, C.1-B through C.1-D, depict conceptual agencies. For C.1-B through C.1-D, the details identifying specific “moving parts” in the diagrams by manufacturer and model are omitted, but it is expected that any agencies producing such documentation will provide diagrams with full manufacturer and model detail for each element of the diagram. Note that the quantities of clients should be documented in order to assist the auditor in understanding the scale of assets and information being protected.

Appendix C.1-B depicts a conceptual state law enforcement agency’s network topology and demonstrates a number of common technologies that are in use throughout the law enforcement community (some of which are compulsory per CJIS policy, and some of which are optional) including Mobile Broadband cards, VPNs, Firewalls, Intrusion Detection Devices, VLANs, and so forth. Note that although most state agencies will likely have highly-available configurations, the example diagram shown omits these complexities and only shows the “major moving parts” for clarity but please note the Policy requires the logical location of all components be shown. The level of detail depicted should provide the reader with a pattern to model future documentation from, but should not be taken as network engineering guidance.

Appendix C.1-C depicts a conceptual county law enforcement agency. A number of common technologies are presented merely to reflect the diversity in the community, including proprietary

Packet-over-RF infrastructures and advanced authentication techniques, and to demonstrate the fact that agencies can act as proxies for other agencies.

Appendix C.1-D depicts a conceptual municipal law enforcement agency, presumably a small one that lacks any precinct-to-patrol data communications. This represents one of the smallest designs that could be assembled that, assuming all other details are properly considered, would meet the criteria for Section 5.7.1.2. This diagram helps to demonstrate the diversity in size that agencies handling criminal justice data exhibit.

Figure C-1-A Overview: Conceptual Connections Between Various Agencies

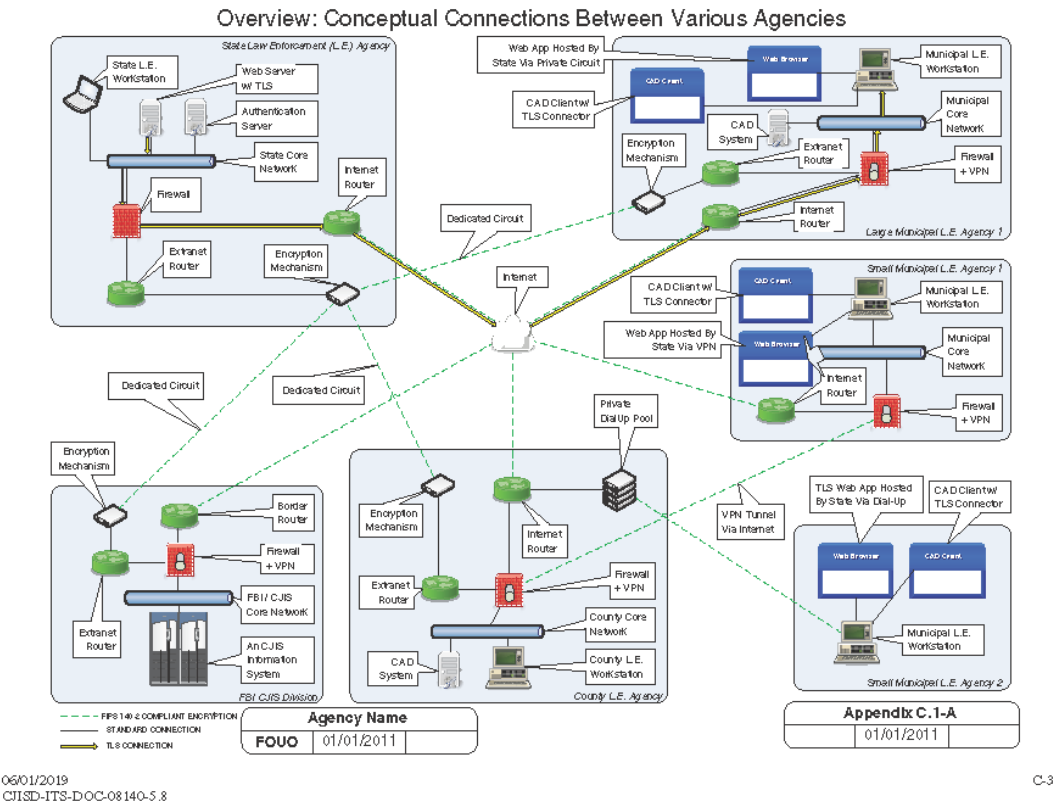
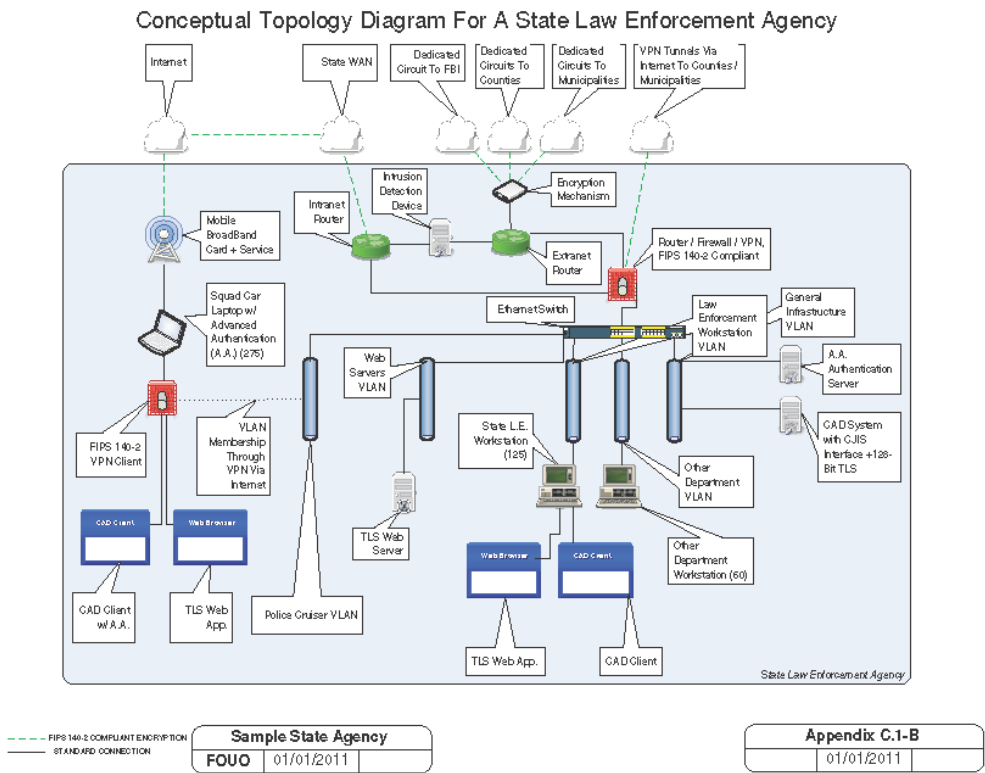


Figure C-1-B Conceptual Topology Diagram for a State Law Enforcement Agency

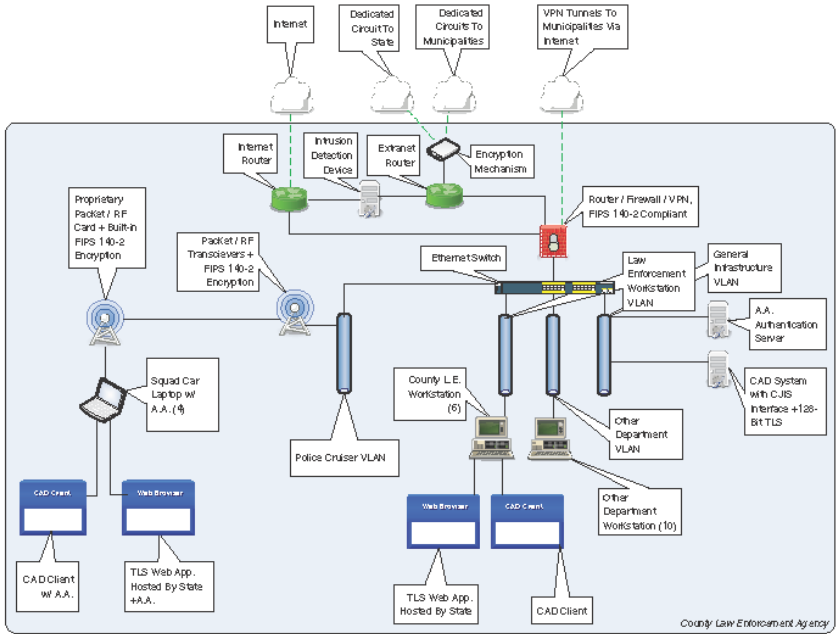


06/01/2019
CIIISD-ITS-DOC-08140-5.8

C-4

Figure C-1-C Conceptual Topology Diagram for a County Law Enforcement Agency

Conceptual Topology Diagram For A County Law Enforcement Agency



--- FIPS 140-2 COMPLIANT ENCRYPTION
— STANDARD CONNECTION

Sample County Agency		
FOUO	01/01/2011	

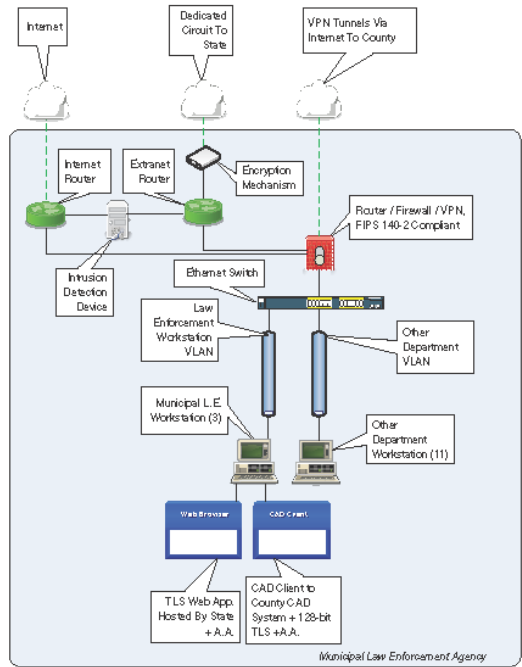
Appendix C.1-C		
	01/01/2011	

06/01/2019
CIISD-ITS-DOC-08140-5.8

C-5

Figure C-1-D Conceptual Topology Diagram for a Municipal Law Enforcement Agency

Conceptual Topology Diagram For A Municipal Law Enforcement Agency



--- FIPS 140-2 COMPLIANT ENCRYPTION
— STANDARD CONNECTION

Sample Municipal Agency		
FOUO	01/01/2011	

06/01/2019
CIIISD-ITS-DOC-08140-5.8

Appendix C.1-D

	01/01/2011	
--	------------	--

C-6

APPENDIX D SAMPLE INFORMATION EXCHANGE AGREEMENTS

D.1 CJIS User Agreement

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS) SYSTEMS USER AGREEMENT

The FBI CJIS Division provides state-of-the-art identification and information services to the local, state, tribal, federal, and international criminal justice communities, as well as the noncriminal justice community, for licensing and employment purposes. These services are administered and maintained by the FBI CJIS Division and managed in cooperation with the CJIS Systems Agency (CSA) and its administrator for CJIS data, the CJIS Systems Officer (CSO). The CJIS Systems include, but are not limited to: the Interstate Identification Index (IIL); National Crime Information Center (NCIC); Uniform Crime Reporting (UCR), whether summary or incident-based reporting to the National Incident-Based Reporting System; Fingerprint Identification Record System; Law Enforcement National Data Exchange (N-DEx); Law Enforcement Enterprise Portal; and the National Instant Criminal Background Check System (NICS).

The FBI CJIS Division provides the following services to its users, as applicable:

1. Operational, technical, and investigative assistance.
2. Telecommunication lines to state, federal, and regulatory interfaces.
3. Legal and legislative review of matters pertaining to all CJIS Systems.
4. Timely information on all aspects of all CJIS Systems and other related programs by means of operating manuals, code manuals, technical and operational updates, various newsletters, information letters, frequently asked questions, and other relevant documents.
5. Training assistance and up-to-date materials provided to each CSO, NICS Point of Contact (POC), state Compact Officer, State Administrator, Information Security Officer (ISO), and other appropriate personnel.
6. Ongoing assistance to Systems' users through meetings and briefings with the CSOs, State Administrators, Compact Officers, ISOs, and NICS State POCs to discuss operational and policy issues.
7. Advisory Process through which authorized users have input as to the policies and procedures governing the operation of CJIS programs.

8. National Crime Prevention and Privacy Compact Administrative Office through which states and other authorized users may submit issues concerning the noncriminal justice use of the III System.
9. Annual NICS Users Conference.
10. Audit.
11. Staff research assistance.

PART 1

The purpose behind a designated CSO is to unify responsibility for Systems user discipline and to ensure adherence to established procedures and policies within each signatory state/territory/tribal agency and by each federal user. This agreement outlines the responsibilities of each CSO as they relate to all CJIS Systems and other related CJIS administered programs. These individuals are ultimately responsible for planning necessary hardware, software, funding, and training for access to all CJIS Systems.

To ensure continued access as set forth above, the CSA agrees to adhere to all applicable CJIS policies including, but not limited to, the following:

1. The signatory state/tribal agency will provide fingerprints that meet submission criteria for all qualifying arrests. In addition, states/tribal agencies will make their records available for interstate exchange for criminal justice and other authorized purposes unless restricted by state/tribal law, and, where applicable, continue to move toward participation in the III and, upon ratification of the National Crime Prevention and Privacy Compact, the National Fingerprint File.
2. Appropriate and reasonable quality assurance procedures; e.g., hit confirmation, audits for record timeliness, and validation, must be in place to ensure that only complete, accurate, and valid information is maintained in the CJIS Systems.
3. Biannual file synchronization of information entered into the III by participating states.
4. Security - Each agency is responsible for appropriate security measures as applicable to physical security of terminals and telecommunication lines; personnel security to include background screening requirements; technical security to protect against unauthorized use; data security to include III use, dissemination, and logging; and security of criminal history

records. Additionally, each CSO must ensure that all agencies establish an information security structure that provides for an ISO and complies with the CJIS Security Policy.

5. Audit - Each agency shall be responsible for complying with all audit requirements for use of CJIS Systems. Each CSO is responsible for completing a triennial audit of all agencies with access to CJIS Systems through the CSO's lines.
6. Training - Each agency shall be responsible for training requirements, including compliance with operator training mandates.
7. Integrity of the Systems - Each agency shall be responsible for maintaining the integrity of the system in accordance with FBI CJIS Division/state/federal/tribal policies to ensure only authorized terminal access; only authorized transaction submission; and proper handling and dissemination of CJI. Each agency shall also be responsible for computer security incident reporting as required by the *CJIS Security Policy*.

The following documents are incorporated by reference and made part of this agreement for CSA users:

1. Bylaws for the CJIS Advisory Policy Board and Working Groups.
2. CJIS Security Policy.
3. Interstate Identification Index Operational and Technical Manual, National Fingerprint File Operations Plan, NCIC 2000 Operating Manual, UCR Handbook-NIBRS Edition, and National Incident-Based Reporting System Volumes 1, 2, and 4.
4. National Crime Prevention and Privacy Compact, 42 United States Code (U.S.C.) §14616.
5. NCIC Standards and UCR Standards, as recommended by the CJIS Advisory Policy Board.
6. The National Fingerprint File Qualification Requirements.
7. Title 28, Code of Federal Regulations, Parts 20 and 25, §50.12, and Chapter IX.
8. Electronic Fingerprint Transmission Specifications.

9. Other relevant documents, to include: NCIC Technical and Operational Updates, CJIS Information Letters, NICS User Manual, NICS Interface Control Document.
10. Applicable federal, state, and tribal laws and regulations.

PART 2

Additionally, there are authorized federal regulatory recipients and other authorized users that provide electronic fingerprint submissions through a CJIS Wide Area Network (WAN) connection (or other approved form of electronic connection) to the CJIS Division that are required to comply with the following CJIS policies:

1. The authorized user will provide fingerprints that meet submission criteria and apply appropriate and reasonable quality assurance procedures.
2. Security - Each agency is responsible for appropriate security measures as applicable to physical security of communication equipment; personnel security to include background screening requirements; technical security to protect against unauthorized use; and security of criminal history records.
3. Audit - Each authorized user shall be responsible for complying with all audit requirements for CJIS Systems. Additionally, each authorized user is subject to a triennial audit by the CJIS Division Audit staff.
4. Training - Each authorized user receiving criminal history record information shall be responsible for training requirements, including compliance with proper handling of criminal history records.

The following documents are incorporated by reference and made part of this agreement for non-CSA authorized users:

1. CJIS Security Policy.
2. National Crime Prevention and Privacy Compact, 42 U.S.C. §14616.
3. Title 28, Code of Federal Regulations, Parts 20 and 25, § 50.12, and Chapter IX.
4. Other relevant documents, to include CJIS Information Letters.

5. Applicable federal, state, and tribal laws and regulations.

GENERAL PROVISIONS

Funding:

Unless otherwise agreed in writing, each party shall bear its own costs in relation to this agreement. Expenditures will be subject to federal and state budgetary processes and availability of funds pursuant to applicable laws and regulations. The parties expressly acknowledge that this in no way implies that Congress will appropriate funds for such expenditures.

Termination:

1. All activities of the parties under this agreement will be carried out in accordance to the above-described provisions.
2. This agreement may be amended or terminated by the mutual written consent of the parties authorized representatives.
3. Either party may terminate this agreement upon 30-days written notification to the other party. Such notice will be the subject of immediate consultation by the parties to decide upon the appropriate course of action. In the event of such termination, the following rules apply:
 - a. The parties will continue participation, financial or otherwise, up to the effective date of termination.
 - b. Each party will pay the costs it incurs as a result of termination.
 - c. All information and rights therein received under the provisions of this agreement prior to the termination will be retained by the parties, subject to the provisions of this agreement.

ACKNOWLEDGMENT AND CERTIFICATION

As a CSO or CJIS WAN Official (or other CJIS authorized official), I hereby acknowledge the duties and responsibilities as set out in this agreement. I acknowledge that these duties and responsibilities have been developed and approved by CJIS Systems users to ensure the reliability, confidentiality, completeness, and accuracy of all information contained in, or obtained by means of, the CJIS Systems. I further acknowledge that failure to comply with these duties and responsibilities may result in the imposition of sanctions against the offending state/agency; other federal, tribal, state, and local criminal justice users; and approved noncriminal justice users with System access, whether direct or indirect. The Director of the FBI (or the National Crime Prevention and Privacy Compact Council), may approve sanctions to include the termination of CJIS services.

I hereby certify that I am familiar with all applicable documents that are made part of this agreement and to all applicable federal and state laws and regulations relevant to the receipt and dissemination of documents provided through the CJIS Systems.

This agreement is a formal expression of the purpose and intent of both parties and is effective when signed. It may be amended by the deletion or modification of any provision contained therein, or by the addition of new provisions, after written concurrence of both parties. The "Acknowledgment and Certification" is being executed by the CSO or CJIS WAN Official (or other CJIS authorized official) in both an individual and representative capacity. Accordingly, this agreement will remain in effect after the CSO or CJIS WAN Official (or other CJIS authorized official) vacates his/her position or until it is affirmatively amended or rescinded in writing. This agreement does not confer, grant, or authorize any rights, privileges, or obligations to any third party.

SYSTEMS USER AGREEMENT

Please execute either Part 1 or Part 2

PART 1

CJIS Systems Officer

Date: _____

Printed Name/Title

CONCURRENCE OF CSA HEAD:

CSA Head

Date: _____

Printed Name/Title

PART 2

CJIS WAN Official (or other CJIS Authorized Official)

Date: _____

Printed Name/Title

CONCURRENCE OF CJIS WAN AGENCY HEAD:

CJIS WAN Agency Head

Date: _____

Printed Name/Title

FBI CJIS DIVISION:

_____ Date: _____
[Name]
Assistant Director
FBI CJIS Division

* The FBI Designated Federal Officer should be notified when a CSO or other CJIS WAN/authorized Official vacates his/her position. The name and telephone number of the Acting CSO or other CJIS WAN/authorized Official, and when known, the name and telephone number of the new CSO or other CJIS WAN/authorized Official, should be provided. Revised: 05/03/2006

D.2 Management Control Agreement

Management Control Agreement

Pursuant to the CJIS Security Policy, it is agreed that with respect to administration of that portion of computer systems and network infrastructure interfacing directly or indirectly with the state network (Network Name) for the interstate exchange of criminal history/criminal justice information, the (Criminal Justice Agency) shall have the authority, via managed control, to set, maintain, and enforce:

- (1) Priorities.
- (2) Standards for the selection, supervision, and termination of personnel access to Criminal Justice Information (CJI).
- (3) Policy governing operation of justice systems, computers, access devices, circuits, hubs, routers, firewalls, and any other components, including encryption, that comprise and support a telecommunications network and related criminal justice systems to include but not limited to criminal history record/criminal justice information, insofar as the equipment is used to process or transmit criminal justice systems information guaranteeing the priority, integrity, and availability of service needed by the criminal justice community.
- (4) Restriction of unauthorized personnel from access or use of equipment accessing the State network.
- (5) Compliance with all rules and regulations of the (Criminal Justice Agency) Policies and CJIS Security Policy in the operation of all information received.

"...management control of the criminal justice function remains solely with the Criminal Justice Agency." Section 5.1.1.4

This agreement covers the overall supervision of all (Criminal Justice Agency) systems, applications, equipment, systems design, programming, and operational procedures associated with the development, implementation, and maintenance of any (Criminal Justice Agency) system to include NCIC Programs that may be subsequently designed and/or implemented within the (Criminal Justice Agency).

John Smith, CIO
Any State Department of Administration

Date

Joan Brown, CIO
(Criminal Justice Agency)

Date

D.3 Noncriminal Justice Agency Agreement & Memorandum of Understanding

MEMORANDUM OF UNDERSTANDING

BETWEEN

THE FEDERAL BUREAU OF INVESTIGATION

AND

(Insert Name of Requesting Organization)

FOR

THE ESTABLISHMENT AND ACCOMMODATION OF
THIRD-PARTY CONNECTIVITY TO THE
CRIMINAL JUSTICE INFORMATION SERVICES DIVISION'S WIDE AREA NETWORK

1. PURPOSE: This Memorandum of Understanding (MOU) between the Federal Bureau of Investigation (FBI) and **(insert requesting organization's name)**, hereinafter referred to as the "parties," memorializes each party's responsibilities with regard to establishing connectivity to records services accessible via the Wide Area Network (WAN) of the FBI's Criminal Justice Information Services (CJIS) Division.

2. BACKGROUND: The requesting organization, **(insert requesting organization's name)**, being approved for access to systems of records accessible via the CJIS WAN, desires connectivity to the CJIS WAN or via a secure Virtual Private Network (VPN) Connection (Internet) to the CJIS WAN. The CJIS Division has created a framework for accommodating such requests based on the type of connection.

In preparing for such non-CJIS-funded connectivity to the CJIS WAN, the parties plan to acquire, configure, and place needed communications equipment at suitable sites and to make electronic connections to the appropriate systems of records via the CJIS WAN.

To ensure that there is a clear understanding between the parties regarding their respective roles in this process, this MOU memorializes each party's responsibilities regarding the development, operation, and maintenance of third-party connectivity to the CJIS WAN. Unless otherwise contained in an associated contract, the enclosed terms apply. If there is a conflict between terms and provisions contained in both the contract and this MOU, the contract will prevail.

3. **AUTHORITY:** The FBI is entering into this MOU under the authority provided by Title 28, United States Code (U.S.C.), Section 534; 42 U.S.C. § 14616; and/or Title 28, Code of Federal Regulations, Part 906.

4. **SCOPE:**

a. The CJIS Division agrees to:

i. Provide the requesting organization with a "CJIS WAN Third-Party Connectivity Package" that will detail connectivity requirements and options compatible with the CJIS Division's WAN architecture upon receipt of a signed nondisclosure statement.

ii. Configure the requesting organization's connection termination equipment suite at Clarksburg, West Virginia, and prepare it for deployment or shipment under the CJIS WAN option. In the Secure VPN arrangement only, the third party will develop, configure, manage, and maintain its network connectivity to its preferred service provider.

iii. Work with the requesting organization to install the connection termination equipment suite and verify connectivity.

iv. Perform installation and/or routine maintenance on the requesting organization's third-party dedicated CJIS WAN connection termination equipment after coordinating with the requesting organization's designated point of contact (POC) and during a time when the CJIS Division's technical personnel are near the requesting organization's site.

v. Perform periodic monitoring and troubleshooting of the requesting organization's CJIS WAN connection termination equipment. Software patches will be maintained on the dedicated CJIS WAN connected network equipment only. Under the Secure VPN option, no availability or data thru-put rates will be guaranteed.

vi. Provide 24 hours a day, 7 days a week uninterrupted monitoring from the CJIS Division's Network Operations Center.

vii. Provide information regarding potential hardware end-of-life replacement cycles to the requesting organization for its budgeting purposes.

viii. Maintain third-party dedicated CJIS WAN connection termination equipment as if in the CJIS Division's operational environment.

ix. Update the appropriate software on the requesting organization's dedicated connection termination equipment connected to the CJIS WAN (i.e., Cisco Internetwork Operating System, SafeNet frame relay encryptor firmware, etc.) pursuant to the requesting organization's authorized maintenance contracts.

x. Provide a POC and telephone number for MOU-related issues.

b. The **(insert requesting organization's name)** agrees to:

i. Coordinate requests for third-party connectivity to the CJIS WAN or the Secure VPN with the CJIS Division's POC.

ii. Purchase hardware and software that are compatible with the CJIS WAN.

iii. Pay for the telecommunications infrastructure that supports its connection to the CJIS WAN or Secure VPN.

iv. Maintain telecommunication infrastructure in support of Secure VPN connectivity.

v. Provide any/all hardware and software replacements and upgrades as mutually agreed to by the parties.

vi. Pay for all telecommunication requirements related to its connectivity.

vii. Provide required information for dedicated service relating to Data Link Connection Identifiers, Circuit Identifier, Permanent Virtual Circuit Identifiers, Local Exchange Carrier Identifier, POC, location, etc., as determined by the parties.

viii. Transport the CJIS WAN connection termination equipment suite to the CJIS Division for configuration and preparation for deployment under the dedicated service option.

ix. Provide registered Internet Protocol information to be used by the requesting organization's system to the CJIS Division.

x. Provide the CJIS Division with six months advance notice or stated amount of time for testing activities (i.e., disaster recovery exercises).

xi. Provide the CJIS Division with applicable equipment maintenance contract numbers and level of service verifications needed to perform software upgrades on connection termination equipment.

xii. Provide the CJIS Division with applicable software upgrade and patch images (or information allowing the CJIS Division to access such images).

xiii. Transport only official, authorized traffic over the Secure VPN.

xiv. Provide a POC and telephone number for MOU-related issues.

5. FUNDING: There are no reimbursable expenses associated with this level of support. Each party will fund its own activities unless otherwise agreed to in writing. This MOU is not an obligation or commitment of funds, nor a basis for transfer of funds, but rather is a basic statement of understanding between the parties hereto of the nature of the relationship for the connectivity efforts. Unless otherwise agreed to in writing, each party shall bear its own costs in relation to this MOU. Expenditures by each party will be subject to its budgetary processes and to the availability of funds and resources pursuant to applicable laws, regulations, and policies. The parties expressly acknowledge that the above language in no way implies that Congress will appropriate funds for such expenditures.

6. SETTLEMENT OF DISPUTES: Disagreements between the parties arising under or relating to this MOU will be resolved only by consultation between the parties and will not be referred to any other person or entity for settlement.

7. SECURITY: It is the intent of the parties that the actions carried out under this MOU will be conducted at the unclassified level. No classified information will be provided or generated under this MOU.

8. AMENDMENT, TERMINATION, ENTRY INTO FORCE, AND DURATION:

a. All activities of the parties under this MOU will be carried out in accordance with the above - described provisions.

b. This MOU may be amended or terminated by the mutual written consent of the parties' authorized representatives.

c. Either party may terminate this MOU upon 30-days written notification to the other party. Such notice will be the subject of immediate consultation by the parties to decide upon the appropriate course of action. In the event of such termination, the following rules apply:

i. The parties will continue participation, financial or otherwise, up to the effective date of the termination.

ii. Each party will pay the costs it incurs as a result of the termination.

iii. All information and rights therein received under the provisions of this MOU prior to the termination will be retained by the parties, subject to the provisions of this MOU.

9. FORCE AND EFFECT: This MOU, which consists of nine numbered sections, will enter into effect upon signature of the parties and will remain in effect until terminated. The parties should review the contents of this MOU annually to determine whether there is a need for the deletion, addition, or amendment of any provision. This MOU is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law or otherwise by any third party against the parties, their parent agencies, the United States, or the officers, employees, agents, or other associated personnel thereof.

The foregoing represents the understandings reached between the parties.

FOR THE FEDERAL BUREAU OF INVESTIGATION

_____	_____
[Name]	Date
Assistant Director	
Criminal Justice Information Services Division	

FOR THE (insert requesting organization name)

_____	_____
Date	

D.4 Interagency Connection Agreement

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS) Wide Area Network (WAN) USER AGREEMENT BY INTERIM REMOTE LATENT USERS

The responsibility of the FBI CJIS Division is to provide state-of-the-art identification and information services to the local, state, federal, and international criminal justice communities, as well as the civil community for licensing and employment purposes. The data provided by the information systems administered and maintained by the FBI CJIS Division are routed to and managed in cooperation with the designated interface agency official. This information includes, but is not limited to, the Interstate Identification Index (III), National Crime Information Center (NCIC), Uniform Crime Reporting (UCR)/National Incident-Based Reporting System (NIBRS), and the Integrated Automated Fingerprint Identification System (IAFIS) programs.

In order to fulfill this responsibility, the FBI CJIS Division provides the following services to its users:

- Operational, technical, and investigative assistance;
- Telecommunications lines to local, state, federal and authorized interfaces;
- Legal and legislative review of matters pertaining to IAFIS, CJIS WAN and other related services;
- Timely information on all aspects of IAFIS, CJIS WAN, and other related programs by means of technical and operational updates, various newsletters, and other relative documents;
- Shared management through the CJIS Advisory Process and the Compact Council;
- Training assistance and up-to-date materials provided to each designated agency official, and;
- Audit.

The concept behind a designated interface agency official is to unify responsibility for system user discipline and ensure adherence to system procedures and policies within each interface agency. These individuals are ultimately responsible for planning necessary hardware, software, funding, training, and the administration of policy and procedures including security and integrity for complete access to CJIS related systems and CJIS WAN related data services by authorized agencies.

The following documents and procedures are incorporated by reference and made part of this agreement:

- *CJIS Security Policy;*
- *Title 28, Code of Federal Regulations, Part 20;*
- Computer Incident Response Capability (CIRC);
- Applicable federal and state laws and regulations.

To ensure continued access as set forth above, the designated interface agency agrees to adhere to all CJIS policies, including, but not limited to, the following:

1. The signatory criminal agency will provide fingerprints for all qualifying arrests either via electronic submission or fingerprint card that meet submission criteria. In addition, the agency will make their records available for interstate exchange for criminal justice and other authorized purposes.
2. The signatory civil agency with legislative authority will provide all qualifying fingerprints via electronic submission or fingerprint card that meet submission criteria.
3. Appropriate and reasonable quality assurance procedures must be in place to ensure that only complete, accurate, and valid information is maintained in the system.
4. Security - Each agency is responsible for appropriate security measures as applicable to physical security of terminals and telecommunications lines; Interim Distributed Imaging System (IDIS) equipment shall remain stand-alone

devices and be used only for authorized purposes; personnel security to meet background screening requirements; technical security to protect against unauthorized use; data security, dissemination, and logging for audit purposes; and actual security of criminal history records. Additionally, each agency must establish an information security structure that provides for an Information Security Officer (ISO) or a security point of contact.

5. Audit - Each agency shall be responsible for complying with the appropriate audit requirements.
6. Training - Each agency shall be responsible for training requirements, including compliance with training mandates.
7. Integrity of the system shall be in accordance with FBI CJIS Division and interface agency policies. Computer incident reporting shall be implemented.

Until states are able to provide remote latent connectivity to their respective latent communities via a state WAN connection, the CJIS Division may provide direct connectivity to IAFIS via a dial-up connection or through the Combined DNA Index System (CODIS) and/or National Integrated Ballistics Information Network (NIBIN) connections. When a state implements a latent management system and is able to provide intrastate connectivity and subsequent forwarding to IAFIS, this agreement may be terminated. Such termination notice will be provided in writing by either the FBI or the state CJIS Systems Agency.

It is the responsibility of the local remote latent user to develop or acquire an IAFIS compatible workstation. These workstations may use the software provided by the FBI or develop their own software, provided it is IAFIS compliant.

The CJIS Division will provide the approved modem and encryptors required for each dial-up connection to IAFIS. The CJIS Communication Technologies Unit will configure and test the encryptors before they are provided to the user. Users requesting remote latent connectivity through an existing CODIS and/or NIBIN connection must receive verification from the FBI that there are a sufficient number of Ethernet ports on the router to accommodate the request.

If at any time search limits are imposed by the CJIS Division, these individual agency connections will be counted toward the total state allotment.

ACKNOWLEDGMENT AND CERTIFICATION

As a CJIS WAN interface agency official serving in the CJIS system, I hereby acknowledge the duties and responsibilities as set out in this agreement. I acknowledge that these duties and responsibilities have been developed and approved by CJIS system users in order to ensure the reliability, confidentiality, completeness, and accuracy of all information contained in or obtained by means of the CJIS system. I further acknowledge that a failure to comply with these duties and responsibilities may subject our agency to various sanctions adopted by the CJIS Advisory Policy Board and approved by the Director of the FBI. These sanctions may include the termination of CJIS service.

As the designated CJIS WAN interface agency official serving in the CJIS system, I hereby certify that I am familiar with the contents of the *Title 28, Code of Federal Regulations, Part 20; CJIS Security Policy; Computer Incident Response Capability*; and applicable federal or state laws and regulations applied to LAFIS and CJIS WAN Programs for the dissemination of criminal history records for criminal and noncriminal justice purposes.

* _____
Signature _____ Print or Type _____

CJIS WAN Agency Official _____ Date _____

CONCURRENCE OF FEDERAL/REGULATORY AGENCY HEAD OR STATE
CJIS SYSTEMS OFFICER (CSO):

* _____
Signature _____ Print or Type _____

* _____
Title _____ Date _____
State CSO _____

FBI CJIS DIVISION:

Signature – [Name]

Assistant Director _____
Title Date

* If there is a change in the CJIS WAN interface agency official, the FBI Designated Federal Employee must be notified in writing 30 days prior to the change.

5/27/2004 UA modification reflects change in CTO title to CSO.

APPENDIX E SECURITY FORUMS AND ORGANIZATIONAL ENTITIES

Online Security Forums / Organizational Entities
AntiOnline
Black Hat
CIO.com
CSO Online
CyberSpeak Podcast
FBI Criminal Justice Information Services Division (CJIS)
Forrester Security Forum
Forum of Incident Response and Security Teams (FIRST)
Information Security Forum (ISF)
Information Systems Audit and Control Association (ISACA)
Information Systems Security Association (ISSA)
Infosyssec
International Organization for Standardization (ISO)
International Information Systems Security Certification Consortium, Inc. (ISC) ²
Metasploit
Microsoft Developer Network (MSDN) Information Security
National Institute of Standards and Technology (NIST)
Open Web Application Security Project (OWASP)
SANS (SysAdmin, Audit, Network, Security) Institute
SC Magazine
Schneier.com
Security Focus
The Register
US Computer Emergency Response Team (CERT)
US DoJ Computer Crime and Intellectual Property Section (CCIPS)

APPENDIX F SAMPLE FORMS

This appendix contains sample forms.

F.1 Security Incident Response Form

**FBI CJIS DIVISION
INFORMATION SECURITY OFFICER (ISO)
SECURITY INCIDENT REPORTING FORM**

NAME OF PERSON REPORTING THE INCIDENT: _____

DATE OF REPORT: _____ (mm/dd/yyyy)

DATE OF INCIDENT: _____ (mm/dd/yyyy)

POINT(S) OF CONTACT (Include Phone/Extension/Email): _____

LOCATION(S) OF INCIDENT: _____

INCIDENT DESCRIPTION: _____

SYSTEM(S) AFFECTED: _____

SYSTEM(S) AFFECTED (e.g. CAD, RMS, file server, etc.): _____

METHOD OF DETECTION: _____

ACTIONS TAKEN/RESOLUTION: _____

Copies To:

John C. Weatherly

(FBI CJIS Division ISO)

1000 Custer Hollow Road

Clarksburg, WV 26306-0102

(304) 625-3660

iso@fbi.gov

APPENDIX G BEST PRACTICES

G.1 Virtualization

Virtualization

This appendix documents security considerations for implementing and operating virtual environments that process, store, and/or transmit Criminal Justice Information.

The FBI CJIS ISO has fielded several inquiries from various states requesting guidance on implementing virtual environments within their data centers. With the proliferation of virtual environments across industry in general there is a realistic expectation that FBI CJIS Auditors will encounter virtual environments during the upcoming year. Criminal Justice Agencies (CJAs) and Noncriminal Justice Agencies (NCJAs) alike need to understand and appreciate the foundation of security protection measures required for virtual environments.

From Microsoft's Introduction to Windows Server 2008

<http://www.microsoft.com/windowsserver2008/en/us/hyperv.aspx>:

"Server virtualization, also known as hardware virtualization, is a hot topic in the IT world because of the potential for serious economic benefits. Server virtualization enables multiple operating systems to run on a single physical machine as virtual machines (VMs). With server virtualization, you can consolidate workloads across multiple underutilized server machines onto a smaller number of machines. Fewer physical machines can lead to reduced costs through lower hardware, energy, and management overhead, plus the creation of a more dynamic IT infrastructure."

From a trade publication, kernelthread.com

<http://www.kernelthread.com/publications/virtualization/>:

"Virtualization is a framework or methodology of dividing the resources of a computer into multiple execution environments, by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing, partial or complete machine simulation, emulation, quality of service, and many others."

From an Open Source Software developer

<http://www.kallasoft.com/pc-hardware-virtualization-basics/>:

"Virtualization refers to virtualizing hardware in software, allowing multiple operating systems, or images, to run concurrently on the same hardware. There are two main types of virtualization software:

- *"Type-1 Hypervisor, which runs 'bare-metal' (on top of the hardware)*
- *"Type-2 Hypervisor which requires a separate application to run within an operating system*

"Type1 hypervisors usually offer the best in efficiency, while Type-2 hypervisors allow for greater support of hardware that can be provided by the operating system. For the developer, power user, and small business IT professionals, virtualization offers the same basic idea of collapsing multiple physical boxes into one. For instance, a small business can run a web server and an Exchange server without the need for two boxes. Developers and power users can use the ability to contain different development environments without the need to modify their main operating system. Big businesses can also benefit from virtualization by allowing software maintenance to be run and tested on a separate image on hardware without having to take down the main production system."

Industry leaders and niche developers are bringing more products to market every day. The following article excerpts, all posted during September 2008, on www.virtualization.com are examples of industry offerings.

"Microsoft and Novell partnered together for joint virtualization solution. Microsoft and Novell are announcing the availability of a joint virtualization solution optimized for customers running mixed-source environments. The joint offering includes SUSE Linux Enterprise Server configured and tested as an optimized guest operating system running on Windows Server 2008 Hyper-V, and is fully supported by both companies' channel partners. The offering provides customers with the first complete, fully supported and optimized virtualization solution to span Windows and Linux environments."

"Sun Microsystems today announced the availability of Sun xVM Server software and Sun xVM Ops Center 2.0, key components in its strategy. Sun also announced the addition of comprehensive services and support for Sun xVM Server software and xVM Ops Center 2.0 to its virtualization suite of services. Additionally, Sun launched xVMserver.org, a new open source community, where developers can download the first source code bundle for Sun xVM Server software and contribute to the direction and development of the product."

"NetEx, specialist in high-speed data transport over TCP, today announced Virtual HyperIP bandwidth optimization solutions for VMware environments that deliver a threefold to tenfold increase in data replication performance. Virtual HyperIP is a software-based Data Transport Optimizer that operates on the VMware ESX server and boosts the performance of storage replication applications from vendors such as EMC, NetApp, Symantec, IBM, Data Domain, and FalconStor. Virtual HyperIP mitigates TCP performance issues that are common when moving data over wide-area network (WAN) connections because of bandwidth restrictions, latency due to distance and/or router hop counts, packet loss and network errors. Like the company's award-winning appliance-based HyperIP, Virtual HyperIP eliminates these issues with an innovative software design developed specifically to accelerate traffic over an IP based network."

From several sources, particularly:

<http://www.windowsecurity.com/articles/security-virtualization.html>

<http://csrc.nist.gov/publications/drafts/6--64rev2/draft-sp800-64-Revision2.pdf>

Virtualization provides several benefits:

- Make better use of under-utilized servers by consolidating to fewer machines saving on hardware, environmental costs, management, and administration of the server infrastructure.
- Legacy applications unable to run on newer hardware and/or operating systems can be loaded into a virtual environment – replicating the legacy environment.
- Provides for isolated portions of a server where trusted and untrusted applications can be ran simultaneously – enabling hot standbys for failover.
- Enables existing operating systems to run on shared memory multiprocessors.
- System migration, backup, and recovery are easier and more manageable.

Virtualization also introduces several vulnerabilities:

- Host Dependent.
- If the host machine has a problem then all the VMs could potentially terminate.
- Compromise of the host makes it possible to take down the client servers hosted on the primary host machine.
- If the virtual network is compromised then the client is also compromised.
- Client share and host share can be exploited on both instances. Potentially this can lead to files being copied to the share that fill up the drive.

These vulnerabilities can be mitigated by the following factors:

- Apply “least privilege” technique to reduce the attack surface area of the virtual environment and access to the physical environment.
- Configuration and patch management of the virtual machine and host, i.e. Keep operating systems and application patches up to date on both virtual machines and hosts.
- Install the minimum applications needed on host machines.
- Practice isolation from host and virtual machine.
- Install and keep updated antivirus on virtual machines and the host.
- Segregation of administrative duties for host and versions.
- Audit logging as well as exporting and storing the logs outside the virtual environment.
- Encrypting network traffic between the virtual machine and host IDS and IPS monitoring.
- Firewall each virtual machine from each other and ensure that only allowed protocols will transact.

G.2 Voice over Internet Protocol

Voice over Internet Protocol (VoIP)

Attribution:

The following information has been extracted from NIST Special Publication 800-58, Security Considerations for Voice over IP Systems.

Definitions:

Voice over Internet Protocol (VoIP) – A set of software, hardware, and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network, or across the Internet.

Internet Protocol (IP) - A protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses.

Summary:

Voice over Internet Protocol (VoIP) has been embraced by organizations globally as an addition to, or replacement for, public switched telephone network (PSTN) and private branch exchange (PBX) telephone systems. The immediate benefits are alluring since the typical cost to operate VoIP is less than traditional telephone services and VoIP can be installed in-line with an organization's existing Internet Protocol services. Unfortunately, installing a VoIP network is not a simple "plug-and-play" procedure. There are myriad security concerns, cost issues with new networking hardware requirements, and overarching quality of service (QoS) factors that have to be considered carefully.

What are some of the advantages of VoIP?

- a. Cost – a VoIP system is usually cheaper to operate than an equivalent office telephone system with a Private Branch Exchange and conventional telephone service.
- b. Integration with other services – innovative services are emerging that allow customers to combine web access with telephone features through a single PC or terminal. For example, a sales representative could discuss products with a customer using the company's web site. In addition, the VoIP system may be integrated with video across the Internet, providing a teleconferencing facility.

What are some of the disadvantages of VoIP?

- a. Startup cost – although VoIP can be expected to save money in the long run, the initial installation can be complex and expensive. In addition, a single standard has not yet emerged for many aspects of VoIP, so an organization must plan to support more than one standard, or expect to make relatively frequent changes as the VoIP field develops.
- b. Security – the flexibility of VoIP comes at a price: added complexity in securing voice and data. Because VoIP systems are connected to the data network, and share many of the same hardware and software components, there are more ways for intruders to attack a VoIP system than a conventional voice telephone system or PBX.

VoIP Risks, Threats, and Vulnerabilities

This section details some of the potential threats and vulnerabilities in a VoIP environment, including vulnerabilities of both VoIP phones and switches. Threat discussion is included because the varieties of threats faced by an organization determine the priorities in securing its communications equipment. Not all threats are present in all organizations. A commercial firm may be concerned primarily with toll fraud, while a government agency may need to prevent disclosure of sensitive information because of privacy or national security concerns. Information security risks can be broadly categorized into the following three types: confidentiality, integrity, and availability, (which can be remembered with the mnemonic “CIA”). Additional risks relevant to switches are fraud and risk of physical damage to the switch, physical network, or telephone extensions.

Packet networks depend for their successful operation on a large number of configurable parameters: IP and MAC (physical) addresses of voice terminals, addresses of routers and firewalls, and VoIP specific software such as Call Managers and other programs used to place and route calls. Many of these network parameters are established dynamically every time a network component is restarted, or when a VoIP telephone is restarted or added to the network. Because there are so many places in a network with dynamically configurable parameters, intruders have a wide array of potentially vulnerable points to attack.

Vulnerabilities described in this section are generic and may not apply to all systems, but investigations by NIST and other organizations have found these vulnerabilities in a number of VoIP systems. In addition, this list is not exhaustive; systems may have security weaknesses that are not included in the list. For each potential vulnerability, a recommendation is included to eliminate or reduce the risk of compromise.

Confidentiality and Privacy

Confidentiality refers to the need to keep information secure and private. For home computer users, this category includes confidential memoranda, financial information, and security information such as passwords. In a telecommunications switch, eavesdropping on conversations is an obvious concern, but the confidentiality of other information on the switch must be protected to defend against toll fraud, voice and data interception, and denial of service attacks. Network IP addresses, operating system type, telephone extension to IP address mappings, and communication protocols are all examples of information that, while not critical as individual pieces of data, can make an attacker’s job easier.

With conventional telephones, eavesdropping usually requires either physical access to tap a line, or penetration of a switch. Attempting physical access increases the intruder's risk of being discovered, and conventional PBXs have fewer points of access than VoIP systems. With VoIP, opportunities for eavesdroppers increase dramatically, because of the many nodes in a packet network.

Switch Default Password Vulnerability

It is common for switches to have a default login/password set, e.g., admin/admin, or root/root. This vulnerability also allows for wiretapping conversations on the network with port mirroring or bridging. An attacker with access to the switch administrative interface can mirror all packets on one port to another, allowing the indirect and unnoticeable interception of all communications. Failing to change default passwords is one of the most common errors made by inexperienced users.

REMEDIATION: If possible, remote access to the graphical user interface should be disabled to prevent the interception of plaintext administration sessions. Some devices provide the option of a direct USB connection in addition to remote access through a web browser interface. Disabling port mirroring on the switch should also be considered.

Classical Wiretap Vulnerability

Attaching a packet capture tool or protocol analyzer to the VoIP network segment makes it easy to intercept voice traffic.

REMEDIATION: A good physical security policy for the deployment environment is a general first step to maintaining confidentiality. Disabling the hubs on IP Phones as well as developing an alarm system for notifying the administrator when an IP Phone has been disconnected will allow for the possible detection of this kind of attack.

ARP Cache Poisoning and ARP Floods

Because many systems have little authentication, an intruder may be able to log onto a computer on the VoIP network segment, and then send ARP commands corrupting ARP caches on sender(s) of desired traffic, then activate IP. An ARP flood attack on the switch could render the network vulnerable to conversation eavesdropping. Broadcasting ARP replies blind is sufficient to corrupt many ARP caches. Corrupting the ARP cache makes it possible to re-route traffic to intercept voice and data traffic.

REMEDIATION: Use authentication mechanisms wherever possible and limit physical access to the VoIP network segment.

Web Server interfaces

Both VoIP switches and voice terminals are likely to have a web server interface for remote or local administration. An attacker may be able to sniff plaintext HTTP packets to gain confidential information. This would require access to the local network on which the server resides.

REMEDIATION: If possible, do not use an HTTP server. If it is necessary to use a web server for remote administration, use the more secure HTTPS (HTTP over SSL or TLS) protocol.

IP Phone Netmask Vulnerability

A similar effect of the ARP Cache Vulnerability can be achieved by assigning a subnet mask and router address to the phone crafted to cause most or all of the packets it transmits to be sent to an attacker's MAC address. Again, standard IP forwarding makes the intrusion all but undetectable.

REMEDIATION: A firewall filtering mechanism can reduce the probability of this attack. Remote access to IP phones is a severe risk.

Extension to IP Address Mapping Vulnerability

Discovering the IP address corresponding to any extension requires only calling that extension and getting an answer. A protocol analyzer or packet capture tool attached to the hub on the dialing instrument will see packets directly from the target instrument once the call is answered. Knowing the IP address of a particular extension is not a compromise in itself, but makes it easier to accomplish other attacks. For example, if the attacker is able to sniff packets on the local network used by the switch, it will be easy to pick out packets sent and received by a target phone. Without knowledge of the IP address of the target phone, the attacker's job may be much more difficult to accomplish and require much longer, possibly resulting in the attack being discovered.

REMEDIATION: Disabling the hub on the IP Phone will prevent this kind of attack. However, it is a rather simple task to turn the hub back on.

Integrity Issues

Integrity of information means that information remains unaltered by unauthorized users. For example, most users want to ensure that bank account numbers cannot be changed by anyone else, or that passwords are changed only by the user or an authorized security administrator. Telecommunication switches must protect the integrity of their system data and configuration. Because of the richness of feature sets available on switches, an attacker who can compromise the system configuration can accomplish nearly any other goal. For example, an ordinary extension could be re-assigned into a pool of phones that supervisors can listen in on or record conversations for quality control purposes. Damaging or deleting information about the IP network used by a VoIP switch results in an immediate denial of service.

The security system itself provides the capabilities for system abuse and misuse. That is, compromise of the security system not only allows system abuse but also allows the elimination of all traceability and the insertion of trapdoors for intruders to use on their next visit. For this reason, the security system must be carefully protected. Integrity threats include any in which system functions or data may be corrupted, either accidentally or as a result of malicious actions. Misuse may involve legitimate users (i.e. insiders performing unauthorized operations) or intruders.

A legitimate user may perform an incorrect, or unauthorized, operations function (e.g., by mistake or out of malice) and may cause deleterious modification, destruction, deletion, or disclosure of switch software and data. This threat may be caused by several factors including the possibility that the level of access permission granted to the user is higher than what the user needs to remain functional.

Intrusion - An intruder may masquerade as a legitimate user and access an operations port of the switch. There are a number of serious intrusion threats. For example, the intruder may use the permission level of the legitimate user and perform damaging operations functions such as:

- Disclosing confidential data
- Causing service deterioration by modifying the switch software
- Crashing the switch
- Removing all traces of the intrusion (e.g., modifying the security log) so that it may not be readily detected

Insecure state - At certain times the switch may be vulnerable due to the fact that it is not in a secure state. For example:

- After a system restart, the old security features may have been reset to insecure settings, and new features may not yet be activated. (For example, all old passwords may have reverted to the default system-password, even though new passwords are not yet assigned.) The same may happen at the time of a disaster recovery.
- At the time of installation the switch may be vulnerable until the default security features have been replaced.

DHCP Server Insertion Attack

It is often possible to change the configuration of a target phone by exploiting the DHCP response race when the IP phone boots. As soon as the IP phone requests a DHCP response, a rogue DHCP server can initiate a response with data fields containing false information.

This attack allows for possible man in the middle attacks on the IP-media gateway, and IP Phones. Many methods exist with the potential to reboot the phone remotely, e.g. “social engineering”, ping flood, MAC spoofing (probably SNMP hooks, etc.).

REMEDIATION: If possible, use static IP addresses for the IP Phones. This will remove the necessity of using a DHCP server. Further, using a state based intrusion detection system can filter out DHCP server packets from IP Phone ports, allowing this traffic only from the legitimate server.

TFTP Server Insertion Attack

It is possible to change the configuration of a target phone by exploiting the TFTP response race when the IP phone is resetting. A rogue TFTP server can supply spurious

information before the legitimate server is able to respond to a request. This attack allows an attacker to change the configuration of an IP Phone.

REMEDIATION: Using a state based intrusion detection system can filter out DHCP server packets from IP Phone ports, allowing such traffic only from the legitimate server. Organizations looking to deploy VoIP systems should look for IP Phone instruments that can download signed binary files.

Availability and Denial of Service

Availability refers to the notion that information and services be available for use when needed. Availability is the most obvious risk for a switch. Attacks exploiting vulnerabilities in the switch software or protocols may lead to deterioration or even denial of service or functionality of the switch. For example: if unauthorized access can be established to any branch of the communication channel (such as a CCS link or a TCP/IP link), it may be possible to flood the link with bogus messages causing severe deterioration (possibly denial) of service. A voice over IP system may have additional vulnerabilities with Internet connections. Because intrusion detection systems fail to intercept a significant percentage of Internet based attacks, attackers may be able to bring down VoIP systems by exploiting weaknesses in Internet protocols and services.

Any network may be vulnerable to denial of service attacks, simply by overloading the capacity of the system. With VoIP the problem may be especially severe, because of its sensitivity to packet loss or delay.

CPU Resource Consumption Attack without any account information.

An attacker with remote terminal access to the server may be able to force a system restart (shutdown all/restart all) by providing the maximum number of characters for the login and password buffers multiple times in succession. Additionally, IP Phones may reboot as a result of this attack.

In addition to producing a system outage, the restart may not restore uncommitted changes or, in some cases, may restore default passwords, which would introduce intrusion vulnerabilities.

REMEDIATION: The deployment of a firewall disallowing connections from unnecessary or unknown network entities is the first step to overcoming this problem. However, there is still the opportunity for an attacker to spoof his MAC and IP address, circumventing the firewall protection.

Default Password Vulnerability

It is common for switches to have a default login/password set, e.g., admin/admin, or root/root. Similarly, VoIP telephones often have default keypad sequences that can be used to unlock and modify network information.

This vulnerability would allow an attacker to control the topology of the network remotely, allowing for not only complete denial of service to the network, but also a port mirroring attack to the attacker's location, giving the ability to intercept any other conversations taking place over the same switch. Further, the switch may have a web server interface, providing an attacker with the ability to disrupt the network without advance knowledge of switch operations and commands. In most systems, telephones download their configuration data on startup using TFTP or similar protocols. The configuration specifies the IP addresses for Call Manager nodes, so an attacker could substitute another IP address pointing to a call manager that would allow eavesdropping or traffic analysis.

REMEDIATION: Changing the default password is crucial. Moreover, the graphical user interface should be disabled to prevent the interception of plaintext administration sessions.

Exploitable software flaws

Like other types of software, VoIP systems have been found to have vulnerabilities due to buffer overflows and improper packet header handling. These flaws typically occur because the software is not validating critical information properly. For example, a short integer may be used as a table index without checking whether the parameter passed to the function exceeds 32,767, resulting in invalid memory accesses or crashing of the system.

Exploitable software flaws typically result in two types of vulnerabilities: denial of service or revelation of critical system parameters. Denial of service can often be implemented remotely, by passing packets with specially constructed headers that cause the software to fail. In some cases the system can be crashed, producing a memory dump in which an intruder can find IP addresses of critical system nodes, passwords, or other security-relevant information. In addition, buffer overflows that allow the introduction of malicious code have been found in VoIP software, as in other applications.

REMEDIATION: These problems require action from the software vendor, and distribution of patches to administrators. Intruders monitor announcements of vulnerabilities, knowing that many organizations require days or weeks to update their software. Regular checking for software updates and patches is essential to reducing these vulnerabilities. Automated patch handling can assist in reducing the window of opportunity for intruders to exploit known software vulnerabilities.

Account Lockout Vulnerability

An attacker will be able to provide several incorrect login attempts at the telnet prompt until the account becomes locked out. (This problem is common to most password-protected systems, because it prevents attackers from repeating login attempts until the correct password is found by trying all possible combinations.)

The account is unable to connect to the machine for the set lockout time.

REMEDIATION: If remote access is not available, this problem can be solved with physical access control.

NIST Recommendations.

Because of the integration of voice and data in a single network, establishing a secure VoIP and data network is a complex process that requires greater effort than that required for data-only networks. In particular, start with these general guidelines, recognizing that practical considerations, such as cost or legal requirements, may require adjustments for the organization:

1. Develop appropriate network architecture.

- Separate voice and data on logically different networks if feasible. Different subnets with separate RFC 1918 address blocks should be used for voice and data traffic, with separate DHCP servers for each, to ease the incorporation of intrusion detection and VoIP firewall protection at the voice gateway, which interfaces with the PSTN, disallow H.323, SIP, or other VoIP protocols from the data network. Use strong authentication and access control on the voice gateway system, as with any other critical network component. Strong authentication of clients towards a gateway often presents difficulties, particularly in key management. Here, access control mechanisms and policy enforcement may help.
- A mechanism to allow VoIP traffic through firewalls is required. There are a variety of protocol dependent and independent solutions, including application level gateways (ALGs) for VoIP protocols, Session Border Controllers, or other standards-based solutions when they mature.
- Stateful packet filters can track the state of connections, denying packets that are not part of a properly originated call. (This may not be practical when multimedia protocol inherent security or lower layer security is applied, e.g., H.235 Annex D for integrity provision or TLS to protect SIP signaling).
- Use IPsec or Secure Shell (SSH) for all remote management and auditing access. If practical, avoid using remote management at all and do IP PBX access from a physically secure system.
- If performance is a problem, use encryption at the router or other gateway, not the individual endpoints, to provide for IPsec tunneling. Since some VoIP endpoints are not computationally powerful enough to perform encryption, placing this burden at a central point ensures all VoIP traffic emanating from the enterprise network has been encrypted. Newer IP phones are able to provide Advanced Encryption System (AES) encryption at reasonable cost. Note that Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, is applicable to all Federal agencies that use cryptographic-based security systems to protect sensitive information in computer

and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106.

2. Ensure that the organization has examined and can acceptably manage and mitigate the risks to their information, system operations, and continuity of essential operations when deploying VoIP systems.

VoIP can provide more flexible service at lower cost, but there are significant tradeoffs that must be considered. VoIP systems can be expected to be more vulnerable than conventional telephone systems, in part because they are tied in to the data network, resulting in additional security weaknesses and avenues of attack (see VoIP Risks, Threats, and Vulnerabilities section for more detailed discussion of vulnerabilities of VoIP and their relation to data network vulnerabilities).

Confidentiality and privacy may be at greater risk in VoIP systems unless strong controls are implemented and maintained. An additional concern is the relative instability of VoIP technology compared with established telephony systems. Today, VoIP systems are still maturing and dominant standards have not emerged. This instability is compounded by VoIP's reliance on packet networks as a transport medium. The public switched telephone network is ultra-reliable. Internet service is generally much less reliable, and VoIP cannot function without Internet connections, except in the case of large corporate or other users who may operate a private network. Essential telephone services, unless carefully planned, deployed, and maintained, will be at greater risk if based on VoIP.

3. Special consideration should be given to E-911 emergency services communications, because E-911 automatic location service is not available with VoIP in some cases.

Unlike traditional telephone connections, which are tied to a physical location, VoIP's packet switched technology allows a particular number to be anywhere. This is convenient for users, because calls can be automatically forwarded to their locations. But the tradeoff is that this flexibility severely complicates the provision of E-911 service, which normally provides the caller's location to the 911 dispatch office. Although most VoIP vendors have workable solutions for E-911 service, government regulators and vendors are still working out standards and procedures for 911 services in a VoIP environment. Agencies must carefully evaluate E-911 issues in planning for VoIP deployment.

4. Agencies should be aware that physical controls are especially important in a VoIP environment and deploy them accordingly.

Unless the VoIP network is encrypted, anyone with physical access to the office LAN could potentially connect network monitoring tools and tap into telephone conversations. Although conventional telephone lines can also be monitored when physical access is obtained, in most offices there are many more points to connect with a LAN without arousing suspicion. Even if encryption is used, physical access to VoIP servers and gateways may allow an attacker to do traffic analysis (i.e., determine which parties are communicating). Agencies therefore should ensure that adequate physical security is in place to restrict access to VoIP network components. Physical security measures, including barriers, locks, access control systems, and guards, are the first line of defense. Agencies must make sure that the proper physical countermeasures are in place to mitigate some of

the biggest risks such as insertion of sniffers or other network monitoring devices. Otherwise, practically speaking this means that installation of a sniffer could result in not just data but all voice communications being intercepted.

5. VoIP-ready firewalls and other appropriate protection mechanisms should be employed. Agencies must enable, use, and routinely test the security features that are included in VoIP systems.

Because of the inherent vulnerabilities (e.g. susceptibility to packet sniffing) when operating telephony across a packet network, VoIP systems incorporate an array of security features and protocols. Organization security policy should ensure that these features are used. In particular, firewalls designed for VoIP protocols are an essential component of a secure VoIP system.

6. If practical, “softphone” systems, which implement VoIP using an ordinary PC with a headset and special software, should not be used where security or privacy are a concern.

Worms, viruses, and other malicious software are extraordinarily common on PCs connected to the internet, and very difficult to defend against. Well-known vulnerabilities in web browsers make it possible for attackers to download malicious software without a user’s knowledge, even if the user does nothing more than visit a compromised web site. Malicious software attached to email messages can also be installed without the user’s knowledge, in some cases even if the user does not open the attachment. These vulnerabilities result in unacceptably high risks in the use of “softphones”, for most applications. In addition, because PCs are necessarily on the data network, using a softphone system conflicts with the need to separate voice and data networks to the greatest extent practical.

7. If mobile units are to be integrated with the VoIP system, use products implementing WiFi Protected Access (WPA), rather than 802.11 Wired Equivalent Privacy (WEP).

The security features of 802.11 WEP provide little or no protection because WEP can be cracked with publicly available software. The more recent WiFi Protected Access (WPA), a snapshot of the ongoing 802.11i standard, offers significant improvements in security, and can aid the integration of wireless technology with VoIP. NIST strongly recommends that the WPA (or WEP if WPA is unavailable) security features be used as part of an overall defense-in-depth strategy. Despite their weaknesses, the 802.11 security mechanisms can provide a degree of protection against unauthorized disclosure, unauthorized network access, or other active probing attacks. However, the Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, is mandatory and binding for Federal agencies that have determined that certain information must be protected via cryptographic means. As currently defined, neither WEP nor WPA meets the FIPS 140-2 standard. In these cases, it will be necessary to employ higher level cryptographic protocols and applications such as secure shell (SSH), Transport Level Security (TLS) or Internet Protocol Security (IPsec) with FIPS 140-2 validated cryptographic modules and associated algorithms to protect information, regardless of whether the nonvalidated data link security protocols are used.

8. Carefully review statutory requirements regarding privacy and record retention with competent legal advisors.

Although legal issues regarding VoIP are beyond the scope of this document, readers should be aware that laws and rulings governing interception or monitoring of VoIP lines, and retention of call records, may be different from those for conventional telephone systems. Agencies should review these issues with their legal advisors. See Section 2.5 for more on these issues.

G.3 Cloud Computing

Cloud Computing

Purpose:

This paper is provided to define and describe cloud computing, discuss CJIS Security Policy (CSP) compliance, detail security and privacy, and provide general recommendations.

Attribution:

- NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing (Dec. 2011)
- NIST SP 800-145, the NIST Definition of Cloud Computing (Sept. 2011)
- NIST SP 800-146, Cloud Computing Synopsis and Recommendations (May 2011)
- CJIS Security Policy, Version 5.0

Definitions and Terms:

Cloud computing – A distributed computing model that permits on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services), software, and information.

Cloud subscriber – A person or organization that is a customer of a cloud

Cloud client – A machine or software application that accesses a cloud over a network connection, perhaps on behalf of a subscriber

Cloud provider – An organization that provides cloud services

Summary:

With many law enforcement agencies looking for ways to attain greater efficiency while grappling with reduced budgets, the idea of cloud computing to maintain data and applications is a viable business solution. But the unique security and legal characteristics of law enforcement agencies means any migration to cloud services may be challenging. Anytime the security of information and transactions must be maintained, as it must be with access to the FBI's CJIS systems and the protection of Criminal Justice Information (CJI), security and policy compliance concerns are bound to arise.

Cloud computing has become a popular and sometimes contentious topic of discussion for both the private and public sectors. This is in part because of the difficulty in describing cloud computing in general terms, because it is not a single kind of system. The “cloud” spans a spectrum of underlying technologies, configuration possibilities, service and deployment models. Cloud computing offers the ability to conveniently rent access to fully featured applications, software development and deployment environments, and computing infrastructure assets - such as network-accessible data storage and processing from a cloud service provider.

One of the benefits of cloud computing is the ability to outsource many of the technical functions agencies may not want to perform for various reasons. Ultimately, the move to cloud computing is a business and security risk decision in which the following relevant factors are given proper consideration:

- readiness of existing applications for cloud deployment
- transition costs
- life-cycle costs
- maturity of service orientation in existing infrastructure
- security and privacy requirements – federal, state, and local

Achieving CJIS Security Policy Compliance:

The question that is often asked is, “Can an Agency be compliant with the CJIS Security Policy and also cloud compute?”

Because the CJIS Security Policy is device and architecture independent (per CSP Section 2.2), the answer is yes, and this can be accomplished— assuming the vendor of the cloud technology is able to meet the existing requirements of the CJIS Security Policy.

There are security challenges that must be addressed if CJIS is to be sent into or through, stored within, or accessed from the cloud.

Admittedly, the existing CJIS Security Policy requirements may be difficult for some cloud-computing vendors due to the sheer numbers and the geographic disbursement of their personnel; however, the requirements aren’t new to vendors serving the criminal justice community and many vendors have been successfully meeting the Policy requirements for years. Even so, they are the minimum security requirements which will provide an acceptable level of assurance that law enforcement and personally identifiable information (PII) will be protected when shared with other law enforcement agencies across the nation.

General CJIS Security Policy Applicability Questions

Before tackling these challenges, the cloud subscriber should first be aware of what security and legal requirements they are subject to prior to entering into any agreement with a cloud provider. Asking the following general questions will help frame the process of determining compliance with the existing requirements of the CJIS Security Policy.

- Will access to Criminal Justice Information (CJI) within a cloud environment fall within the category of remote access? (5.5.6 Remote Access)
- Will advanced authentication (AA) be required for access to CJI within a cloud environment? (5.6.2.2 Advanced Authentication, 5.6.2.2.1 Advanced Authentication Policy and Rationale)
- Does/do any cloud service provider's datacenter(s) used in the transmission or storage of CJI meet all the requirements of a physically secure location? (5.9.1 Physically Secure Location)
- Are the encryption requirements being met? (5.10.1.2 Encryption)
 - Who will be providing the encryption as required in the CJIS Security Policy (client or cloud service provider)? *Note: individuals with access to the keys can decrypt the stored files and therefore have access to unencrypted CJI.*
 - Is the data encrypted while at rest and in transit?
- What are the cloud service provider's incident response procedures? (5.3 Policy Area 3: Incident Response)
 - Will the cloud subscriber be notified of any incident?
 - If CJI is compromised, what are the notification and response procedures?
- Is the cloud service provider a private contractor/vendor?
 - If so, they are subject to the same screening and agreement requirements as any other private contractors hired to handle CJI? (5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum; 5.12.1.2 Personnel Screening for Contractors and Vendors)
- Will the cloud service provider allow the CSA and FBI to conduct compliance and security audits? *Note: Cloud facilities such as datacenters in which CJI will be stored or processed should be audited as would any other datacenter housing and processing CJI.* (5.11.1 Audits by the FBI CJIS Division; 5.11.2 Audits by the CSA)

- How will event and content logging be handled? (5.4 Policy Area 4, Auditing and Accountability)
 - Will the cloud service provider handle the events and content logging required by the CJIS Security Policy and provide that upon request?
 - What are the cloud service provider's responsibilities with regard to media protection and destruction? (5.8 Policy Area 8: Media Protection)

Ultimately, the goal is to remain committed to using technology in its information sharing processes, but not at the sacrifice of the security of the information with which it has been entrusted. As stated in the CJIS Security Policy, device and architecture independence permits the use of cloud computing, but the security requirements do not change.

Cloud Utilization Scenarios

1. Encrypted CJI in a Cloud Environment–Key Management Control, Security Awareness Training, and Personnel Controls

Prior to permitting CJI to be stored or traverse through a cloud environment, the agency should ensure proper encryption key management control procedures are implemented to determine who has access and control over the encryption keys. Proper key management control is vital to CJI security as those individuals (agency or cloud employees) with access to the keys can decrypt the stored files, and therefore, have unescorted access to unencrypted CJI. This means all those individuals must be subjected to security awareness training (CJIS Security Policy section 5.2) and must meet personnel security (CJIS Security Policy Section 5.12) requirements as individuals with unescorted access to unencrypted CJI.

Note: As a best security practice, the CJIS ISO Program does not recommend allowing the cloud service provider access to the encryption keys used to protect CJI. However, it may not always be reasonable to expect the agency, criminal justice or noncriminal justice, to accomplish this task.

- a. Scenario 1–Agency Stores CJI in a Cloud:

A CJA stores encrypted CJI (Backup files and drives) in a cloud service provider's environment. To access CJI, the agency will extract the CJI from the cloud to its local machine, and then decrypt the CJI. The CJI is processed, re-encrypted, and then re-uploaded to the cloud environment for storage. In this scenario, the agency always encrypts the CJI prior to placing it in the cloud and only authorized users of the agency have access to the encryption keys. Since the agency maintains the encryption keys, the cloud service provider employees would not need to undergo fingerprint-based background checks, nor have security awareness training. These requirements are negated, because only authorized personnel with access to the keys have the ability to view this CJI in an unencrypted form.

- b. Scenario 2–Agency Accesses CJI While in a Cloud:

A CJA stores CJI (files and drives) in a cloud service provider's environment, but as part of daily operations authorized users will remotely access the encrypted CJI in the cloud. The user will decrypt the CJI while it is in the cloud's virtual environment, process the data, and then re-encrypt the data prior to ending the remote session. The agency maintains the keys and the cloud service provider does not have access to the encryption keys. However, since the CJI is decrypted within the cloud's virtual environment, any administrative personnel employed by the cloud provider having the ability to access the virtual environment must be identified and subjected to security awareness training and personnel security controls as described in the CJIS Security Policy.

c. Scenario 3–CJI Impact from a Cloud Datacenter Critical Systems Crash–Core Dump²
Recovery:

A CJA utilizes a cloud service provider (IaaS or PaaS) to store CJI and remotely accesses the environment to process CJI. During normal operation, the cloud provider experiences systems outages within the datacenter in which CJI is processed and stored. The cloud provider's administrators need to repair the systems and restore service using data from a core dump to return to normal operations. The cloud service provider as part of the Service Level Agreement (SLA) with the CJA has been authorized to maintain the encryption keys in order respond to such an event. The cloud administrators with such access have underwent fingerprint-based background checks and security awareness training. This allows the cloud administrators to decrypt CJI so that it is written to the core dump files for restoration following the system outage. CJI, however, is encrypted at all times except when part of the core dump files. As part of the SLA, the cloud service provider has agreed to treat the core dump files as CJI to ensure all protection are in place in compliance with the CJIS Security Policy.

Note: Writing encrypted data to a core dump corrupts the data and makes it unusable because the key no longer decrypts the data. This is problematic when attempting to recover encrypted data written to a core dump. The CJA could have ensured the cloud provider exclude encrypted data (CJI) from the core dump, but chose against it.

The Cloud Model Explained:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

² Core Dump - A file of a computer's documented memory of when a program or computer crashed. The file consists of the recorded status of the working memory at an explicit time, usually close to when the system crashed or when the program ended atypically as it presents the risk that the system failure would ensure the loss of the encrypted data.

The cloud model as defined by NIST consists of five essential characteristics, offers the option of three service models, and may be deployed via any of four deployment models as shown in Figure 1 below:

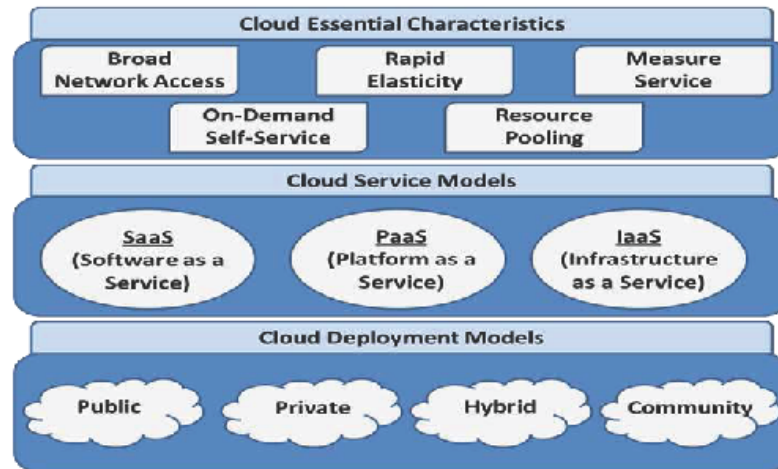


Figure 1 - Visual Depiction of the NIST Cloud Computing Definition

Essential Characteristics:

On-demand self-service

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in which the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction

(e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity

Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service

Cloud systems automatically control and optimize resource use by leveraging a metering capability* at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

** Typically this is done on a pay-per-use or charge-per-use basis.*

Deployment Models:

Private cloud

The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud

The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud

The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud

The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Service Models:

Software as a Service (SaaS)

This model provides the consumer the capability to use the provider's applications running on a cloud infrastructure*.

** A cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.*

The SaaS service model is often referred to as "Software deployed as a hosted service and accessed over the Internet."

The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface.

When using the SaaS service model it should be understood that the consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Platform as a Service (PaaS)

This model provides the consumer the capability to deploy consumer-created or acquired applications* created using programming languages, libraries, services, and tools supported by the provider onto the cloud infrastructure.

** This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources.*

When using the PaaS service model the consumer may have control over the deployed applications and possibly configuration settings for the application-hosting environment, but does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage.

Infrastructure as a Service (IaaS)

This model provides the consumer the capability to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, including operating systems and applications.

When using the IaaS service model the consumer may have control over operating systems, storage, and deployed applications; and possibly limited control of select

networking components (e.g., host firewalls), but does not manage or control the underlying cloud infrastructure.

Key Security and Privacy Issues:

Although the emergence of cloud computing is a recent development, insights into critical aspects of security can be gleaned from reported experiences of early adopters and also from researchers analyzing and experimenting with available cloud provider platforms and associated technologies. The sections below highlight privacy and security-related issues that are believed to have long-term significance for public cloud computing and, in many cases, for other cloud computing service models.

Because cloud computing has grown out of an amalgamation of technologies, including service oriented architecture, virtualization, Web 2.0, and utility computing, many of the privacy and security issues involved can be viewed as known problems cast in a new setting. The importance of their combined effect in this setting, however, should not be discounted. Public cloud computing does represent a thought-provoking paradigm shift from conventional norms to an open organizational infrastructure—at the extreme, *displacing applications from one organization's infrastructure to the infrastructure of another organization, where the applications of potential adversaries may also operate.*

Governance

Governance implies control and oversight by the organization over policies, procedures, and standards for application development and information technology service acquisition, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services. With the wide availability of cloud computing services, lack of organizational controls over employees engaging such services arbitrarily can be a source of problems. While cloud computing simplifies platform acquisition, it doesn't alleviate the need for governance; instead, it has the opposite effect, amplifying that need.

Dealing with cloud services requires attention to the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met. Ensuring systems are secure and risk is managed is challenging in any environment and even more daunting with cloud computing. Audit mechanisms and tools should be in place to determine how data is stored, protected, and used, to validate services, and to verify policy enforcement. A risk management program should also be in place that is flexible enough to deal with the continuously evolving and shifting risk landscape.

Compliance

Compliance refers to an organization's responsibility to operate in agreement with established laws, regulations, standards, and specifications. Various types of security and privacy laws and regulations exist within different countries at the national, state, and local levels, making compliance a potentially complicated issue for cloud computing.

Law and Regulations

Cloud providers are becoming more sensitive to legal and regulatory concerns, and may be willing to commit to store and process data in specific jurisdictions and apply required safeguards for security and privacy. However, the degree to which they will accept liability in their service agreements, for exposure of content under their control, remains to be seen. Even so, organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.

Data Location

One of the most common compliance issues facing an organization is data location. A characteristic of many cloud computing services is that data is stored redundantly in multiple physical locations and detailed information about the location of an organization's data is unavailable or not disclosed to the service consumer. This situation makes it difficult to ascertain whether sufficient safeguards are in place and whether legal and regulatory compliance requirements are being met. External audits and security certifications can alleviate this issue to some extent, but they are not a panacea.

When information crosses borders, the governing legal, privacy, and regulatory regimes can be ambiguous and raise a variety of concerns. Consequently, constraints on the trans-border flow of sensitive data, as well as the requirements on the protection afforded the data, have become the subject of national and regional privacy and security laws and regulations.

Electronic Discovery

The capabilities and processes of a cloud provider, such as the form in which data is maintained and the electronic discovery-related tools available, affect the ability of the organization to meet its obligations in a cost effective, timely, and compliant manner. A cloud provider's archival capabilities may not preserve the original metadata as expected, causing spoliation (i.e., the intentional, reckless, or negligent destruction, loss, material alteration, or obstruction of evidence that is relevant to litigation), which could negatively impact litigation.

Trust

Under the cloud computing paradigm, an organization relinquishes direct control over many aspects of security and privacy, and in doing so, confers a high level of trust onto the cloud provider. At the same time, federal agencies have a responsibility to protect information and information systems commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction, regardless of whether the information is collected or maintained by or on behalf of the agency; or whether the information systems are used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency

Insider Access

Data processed or stored outside the physical confines of an organization, its firewall, and other security controls bring with it an inherent level of risk. The insider security threat is a well-known issue for most organizations. Incidents may involve various types of fraud, sabotage of information resources, and theft of sensitive information.

Data Ownership

The organization's ownership rights over the data must be firmly established in the service contract to enable a basis for trust and privacy of data. The continuing controversy over privacy and data ownership rights for social networking users illustrates the impact that ambiguous terms can have on the parties involved.

Ideally, the contract should state clearly that the organization retains exclusive ownership over all its data; that the cloud provider acquires no rights or licenses through the agreement, including intellectual property rights or licenses, to use the organization's data for its own purposes; and that the cloud provider does not acquire and may not claim any interest in the data due to security. For these provisions to work as intended, the terms of data ownership must not be subject to unilateral amendment by the cloud provider.

Visibility

Continuous monitoring of information security requires maintaining ongoing awareness of security controls, vulnerabilities, and threats to support risk management decisions. Transition to public cloud services entails a transfer of responsibility to the cloud provider for securing portions of the system on which the organization's data and applications operate.

Ancillary Data

While the focus of attention in cloud computing is mainly on protecting application data, cloud providers also hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks.

Risk Management

Assessing and managing risk in systems that use cloud services can be a challenge. With cloud-based services, some subsystems or subsystem components fall outside of the direct control of a client organization. Many organizations are more comfortable with risk when they have greater control over the processes and equipment involved. Establishing a level of trust about a cloud service is dependent on the degree of control an organization is able to exert on the provider to provision the security controls necessary to protect the organization's data and applications, and also the evidence provided about the effectiveness of those controls. Ultimately, if the level of trust in the service falls below expectations and the organization is unable to employ compensating controls, it must either reject the service or accept a greater degree of risk.

Architecture

The architecture of the software and hardware used to deliver cloud services can vary significantly among public cloud providers for any specific service model. It is important to understand the technologies the cloud provider uses to provision services and the implications the technical controls involved have on security and privacy of the system throughout its lifecycle. With such information, the underlying system architecture of a cloud can be decomposed and mapped to a framework of security and privacy controls that can be used to assess and manage risk.

Identity and Access Management

Data sensitivity and privacy of information have become increasingly an area of concern for organizations. The identity proofing and authentication aspects of identity management entail the use, maintenance, and protection of PII collected from users. Preventing unauthorized access to information resources in the cloud is also a major consideration. One recurring issue is that the organizational identification and authentication framework may not naturally extend into a public cloud and extending or changing the existing framework to support cloud services may prove difficult.

Software Isolation

High degrees of multi-tenancy over large numbers of platforms are needed for cloud computing to achieve the envisioned flexibility of on-demand provisioning of reliable services and the cost

benefits and efficiencies due to economies of scale. Regardless of the service model and multi-tenant software architecture used, the computations of different consumers must be able to be carried out in isolation from one another, mainly through the use of logical separation mechanisms.

Data Protection

Data stored in a public cloud typically resides in a shared environment collocated with data from other customers. Organizations placing sensitive and regulated data into a public cloud, therefore, must account for the means by which access to the data is controlled and the data is kept secure. Similar concerns exist for data migrated within or between clouds.

Value Concentration

Having data collocated with that of an organization with a high threat profile could also lead to a denial of service, as an unintended casualty from an attack targeted against that organization. Similarly, side effects from a physical attack against a high profile organization's cloud-based resources are also a possibility. For example, over the years, facilities of the Internal Revenue Service have attracted their share of attention from would-be attackers.

Data Isolation

Database environments used in cloud computing can vary significantly. Accordingly, various types of multi-tenant arrangements exist for databases. Each arrangement pools resources differently, offering different degrees of isolation and resource efficiency. Regardless of implementation decision, data must be secured while at rest, in transit, and in use, and access to the data must be controlled.

Data Sanitization

The data sanitization practices that a cloud provider implements have obvious implications for security. Sanitization involves the expunging of data from storage media by overwriting, degaussing, or other means, or the destruction of the media itself, to prevent unauthorized disclosure of information. Data sanitization also applies to backup copies made for recovery and restoration of service and residual data remaining upon termination of service.

In a public cloud computing environment, data from one consumer is physically collocated (e.g., in an IaaS data store) or commingled (e.g., in a SaaS database) with the data of other consumers, which can complicate matters. Service agreements should stipulate sufficient measures that are taken to ensure data sanitization is performed appropriately throughout the system lifecycle.

Encryption

Client end-to-end encryption (e.g. encryption/decryption occurs on the law enforcement controlled client prior to data entering the cloud and decryption occurs only on the client device after encrypted data is removed from the cloud service) with cryptographic keys managed solely by law enforcement would prevent exposure of sensitive data.

- May cause significant cloud service functionality limitations on available service types made available for sensitive data. This may also increase expense to cover key items, such as key management and client software. Additionally, a number of specific SLA or contract clauses may be necessary for the implementation of client end-to-end encryption.

Use of cloud services without end-to-end encryption implemented by the client is another option that would require cloud service provider participation in the encryption of data.

- This would require at least some cloud provider personnel to undergo personnel background screening and training.
- Specialized Service Level Agreements (SLA) and/or contractual clauses would be necessary to identify those personnel that may have access to unencrypted, sensitive data.
- Conducting the analysis and gaining approval of particular cloud service implementations not utilizing end-to-end encryption for sensitive law enforcement data may be costly and time consuming due to the high degree of technical complexity.

Availability

In simple terms, availability is the extent to which an organization's full set of computational resources is accessible and usable. Denial of service attacks, equipment outages, and natural disasters are all threats to availability. The concern is that most downtime is unplanned and can impact the mission of the organization. Some examples of unplanned service interruptions that cause concerns are:

- Temporary Outages
- Prolonged and Permanent Outages
- Denial of Service

Incident Response

The complexity of a cloud service can obscure recognition and analysis of incidents. Revising an organization's incident response plan to address differences between the organizational computing environment and a cloud computing environment is an important, but easy-to-overlook prerequisite to transitioning applications and data.

Data Availability

The availability of relevant data from event monitoring is essential for timely detection of security incidents. Cloud consumers are often confronted with extremely limited capabilities for detection of incidents in public cloud environments. The situation varies among cloud service models and cloud providers. For example, PaaS providers typically do not make event logs available to consumers, who are then left mainly with event data from self-deployed applications (e.g., via application logging). Similarly, SaaS consumers are completely dependent upon the cloud provider to provide event data such as activity logging, while IaaS consumers control more of the information stack and have access to associated event sources.

Incident Analysis and Resolution

An analysis to confirm the occurrence of an incident or determine the method of exploit needs to be performed quickly and with sufficient detail of documentation and care to ensure that traceability and integrity is maintained for subsequent use, if needed (e.g., a forensic copy of incident data for legal proceedings). Issues faced by cloud consumers when performing incident analysis include lack of detailed information about the architecture of the cloud relevant to an incident, lack of information about relevant event and data sources held by the cloud provider, ill-defined or vague incident handling responsibilities stipulated for the cloud provider, and limited capabilities for gathering and preserving pertinent data sources as evidence. Understanding and negotiating the provisions and procedures for incident response should be done before entering into a service contract, rather than as an afterthought.

General Recommendations:

A number of significant security and privacy issues were covered in the previous subsections. Table 1 summarizes those issues and related recommendations for organizations to follow when planning, reviewing, negotiating, or initiating a public cloud service outsourcing arrangement.

Table 1: Security and Privacy Issue Areas and Recommendations

Areas	Recommendations
Governance	<ul style="list-style-type: none"> Extend organizational practices pertaining to the policies, procedures, and standards used for application development and service provisioning in the cloud, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services. Put in place audit mechanisms and tools to ensure organizational practices are followed throughout the system lifecycle.
Compliance	<ul style="list-style-type: none"> Understand the various types of laws and regulations that impose security and privacy obligations on the organization and potentially impact cloud computing initiatives, particularly those involving data location, privacy and security controls, records management, and electronic discovery requirements. Review and assess the cloud provider's offerings with respect to the organizational requirements to be met and ensure that the contract terms adequately meet the requirements. Ensure that the cloud provider's electronic discovery capabilities and processes do not compromise the privacy or security of data and applications.
Trust	<ul style="list-style-type: none"> Ensure that service arrangements have sufficient means to allow visibility into the security and privacy controls and processes employed by the cloud provider, and their performance over time. Establish clear, exclusive ownership rights over data. Institute a risk management program that is flexible enough to adapt to the constantly evolving and shifting risk landscape for the lifecycle of the system. Continuously monitor the security state of the information system to support on-going risk management decisions.
Architecture	<ul style="list-style-type: none"> Understand the underlying technologies that the cloud provider uses to provision services, including the implications that the technical controls involved have on the security and privacy of the system, over the full system lifecycle and across all system components.
Identity and Access Management	<ul style="list-style-type: none"> Ensure that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions, and are suitable for the organization.
Software Isolation	<ul style="list-style-type: none"> Understand virtualization and other logical isolation techniques that the cloud provider employs in its multi-tenant software architecture, and assess the risks involved for the organization.
Data Protection	<ul style="list-style-type: none"> Evaluate the suitability of the cloud provider's data management solutions for the organizational data concerned and the ability to control access to data, to secure data while at rest, in transit, and in use, and to sanitize data.

	<ul style="list-style-type: none">• Take into consideration the risk of collating organizational data with that of other organizations whose threat profiles are high or whose data collectively represent significant concentrated value.• Fully understand and weigh the risks involved in cryptographic key management with the facilities available in the cloud environment and the processes established by the cloud provider.
Availability	<ul style="list-style-type: none">• Understand the contract provisions and procedures for availability, data backup and recovery, and disaster recovery, and ensure that they meet the organization's continuity and contingency planning requirements.• Ensure that during an intermediate or prolonged disruption or a serious disaster, critical operations can be immediately resumed, and that all operations can be eventually reinstituted in a timely and organized manner.
Incident Response	<ul style="list-style-type: none">• Understand the contract provisions and procedures for incident response and ensure that they meet the requirements of the organization.• Ensure that the cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident.• Ensure that the organization can respond to incidents in a coordinated fashion with the cloud provider in accordance with their respective roles and responsibilities for the computing environment.

G.4 Mobile Appendix

Mobile Appendix

Introduction

Mobile devices present a unique security challenge with regard to the correct application of CJIS Security Policy requirements. This appendix is intended to provide best practices based on industry standards and on methods to achieve policy compliance in mobile device employment scenarios. The technical methods used to achieve compliance with CJIS Security Policy will typically be different within the mobile environment than those used in fixed locations. Many of the security features and capabilities inherited by endpoint devices from the fixed environment are either not present or present in a different form in the mobile environment. Additionally, the basic technologies used in some types of mobile devices may adequately fulfill some of the CJIS Security Policy requirements which would require additional software or added features in a traditional fixed computing environment. Due to the complexity and rapid evolution of the mobile environment, this Appendix will remain as device and vendor agnostic as practical, however certain key requirements for specific mobile operating systems will be identified for the major mobile operating systems (e.g. Apple iOS, Android) as the underlying technologies are fundamentally different and offer different levels of built-in compliance to CJIS Security Policy.

Sections within this appendix will provide recommendations regarding priorities and level of effort versus value of applying certain security controls in the mobile environment. These recommendations do not supersede or modify the requirements listed in the CJIS Security Policy, and are intended to describe the effect of inherent security functions and inherent device limitations in many mobile platforms that impact the application of policy elements in the mobile environment.

Mobile Device Risk Scenarios

There are multiple risk scenarios that may apply to mobile devices depending on the category of device (e.g. Laptop, Tablet, and 'Pocket sized' devices such as smartphones) and the methods of device connectivity (e.g. cellular service, WiFi + Cellular, WiFi only). Device category and method of connection define the technology types within the device which inherently affects the total level of compliance with CJIS Security Policy that can be obtained by the mobile device.

It is advisable for acquiring agencies to review the mobile device guidance in this Appendix prior to completing selection and acquisition of particular devices. Both the device category and connectivity methods installed and configured on the device will impact the overall risk scenario associated with the device and may significantly affect the effective cost to bring use of the device in compliance with the CJIS Security Policy. For instance, inclusion of cellular radios with the ability to remotely control a device significantly changes the risk scenario by allowing remote tracking, file deletion, and device management which could provide a higher level of CJIS Security Policy compliance than a WiFi only device that does not guarantee the ability to remotely manage the device. However, inclusion of cellular technology may significantly increase the initial device costs and incur ongoing subscription costs. Appropriate choices based on the intended use of the device along with the types and methods of Criminal Justice Information (CJI) data to be accessed could greatly reduce agency cost and enhance security.

Device Categories

This appendix defines risk levels for three categories of devices. Prior to reading individual sections of this Appendix, the agency should identify which device categories will apply to their employment scenario. If multiple categories of devices are employed, individual technical configurations and local policy will likely need to be defined for each category of device based on the risk inherent in the technical characteristics associated with each device category.

Laptop devices

The laptop device category includes mobile devices in a larger format that are transported either in a vehicle mount or a carrying case and include a monitor with attached keyboard. This includes all traditional laptop computers that utilize a 'traditional', full featured operating system (e.g. Windows or a Linux variant). Also included in this category are 'tablet' type full featured computers running a traditional full featured operating system but without an attached keyboard. The main defining factor is the use of a full featured operating system and a form factor too large to be carried in a pocket. In general, devices of this type connect via WiFi only, but may include an internal cellular access card in some cases.

The risks associated with this device type are similar to a standard desktop computer at the technical level, but are increased due to the potential to connect directly to the internet without the benefit of organizational network security layers (e.g. network firewall, IDS/IPS, network monitoring devices). There is also an increased risk of intentional device theft from vehicles or unsecure locations as these devices are too large to be carried on the authorized user's body. There may be increased risk from the limited technical ability to wipe or track a lost/stolen device depending on the particular technical means used for remote device connectivity (e.g. cellular or WiFi).

In general, the technical configurations for compliance with most of the CJIS Security Policy that is accomplished via the operating system (e.g. auditing, access control, etc) will remain consistent with normal fixed location computing systems for laptop devices, but some functions may operate in an unexpected manner due to lack of constant connectivity. Thorough testing of applied security policy elements within the expected mobile environments will help ensure the applied policy configurations remain effective and appropriate when applied to mobile laptop devices.

NOTE: Some newer devices running multi-function operating systems (e.g. Windows 8 or similar multi-mode operating systems) may exhibit technical features associated with both laptop and tablet device categories based on their current operating mode which may be reconfigured by the user on demand. If this is the case, it will be necessary to assess and configure multiple operating modes to be compliant with CJIS Security Policy on the device, or restrict the operating mode to one category of operation.

Tablet devices

The tablet device category includes larger format devices transported via vehicle mount or portfolio sized carry case that typically consist of a touch screen without attached keyboard. These devices utilize a limited feature operating system (e.g. Apple iOS, Google Android, Windows mobile) that is inherently more resistant than a traditional operating system to certain types of network based technical attacks due to the limited feature sets. Additionally, limited functionality operating systems are designed specifically for the mobile environment where battery life and power efficiency are primary design drivers. This inherently limits the types of services that can

function effectively on the devices (e.g. traditional real-time anti-virus software) as the base operating system may not be designed to allow installed applications enhanced execution priority in the background and or the ability to examine the contents or communications associated within another application. However, this same design methodology significantly limits the vectors available for malware transmission and the device or application data actually accessible to malware if a device becomes infected.

Tablet devices will have different risks associated depending on the installed and configured methods for network access (e.g. 'always on cellular' vs. WiFi only). Physical risks associated with this category are similar to the laptop category for enhanced likelihood of intentional theft or device hijacking while unattended, while the technical risks are similar to the pocket device category.

Pocket devices/Handheld devices

The pocket/handheld device category is technically similar or identical to the tablet category and is primarily differentiated by device form factor. Pocket/handheld devices are characterized as having a limited functionality operating system and a small form factor intended for carry in a pocket or 'holster' attached to the body. The bulk of this category will be cellular 'smartphones' with integrated cellular data connectivity, however devices intended to be worn or carried on the body (e.g. portable fingerprint devices) may also be included in this category if they operate using a limited functionality operating system. Custom or specialty devices may meet the form factor distinction for this category, but operate using a full feature operating system. In rare cases of this nature the employing agency should apply security guidance and principles in this appendix for both the laptop and pocket device categories.

Risks associated with this category are a reduced threat of theft to a stored devices (e.g. device left unattended in a vehicle) since these devices are typically carried continuously by the authorized user, but include a greater risk of temporary or permanent loss of control due to the device being misplaced by the authorized user.

Due to the installation of a limited functionality operating system, the technical threat to these devices via a network based attack is significantly lower than the laptop category, however, the threat of unauthorized access at the device level may be higher if the device is lost due to technical limits on multi-factor authentication to the operating system itself and practical limits to device passwords due to screen/software keyboard limitations.

NOTE: Data accessible on pocket or tablet devices simply through the entry of a single device PIN or password should not be considered secure due to the likelihood of enhanced password guessing based on fingerprints/smudges on the device touch screen. Any data stored on devices of these types should be protected within a separate secure container using Advanced Authentication.

Device Connectivity

There are three main categories of device connectivity that are associated with varying risk levels and threats to the devices. The Three categories are: Cellular Network Only (always on), WiFi Only (includes 'on demand' cellular), and Cellular (always on) + WiFi network. The risks associated with connectivity categories are general risks and may apply differently to any particular device at different points in its usage or lifecycle. Particular device configurations either through the operating system or a third-party mobile device management (MDM) system may be

able to significantly control and define which particular connectivity risks may be associated with a particular device.

Cellular Network Only (always on)

Cellular network connectivity is characterized by 'always on' network connection through the device internal radio to a cellular network provider. There is a reasonable assurance that devices with 'always on' cellular can be tracked, managed, or wiped remotely if lost or stolen. This will significantly reduce risks associated with loss of the device and attempted illicit access to the device. One important consideration for this risk category is characterization of the device as 'always on' or 'on demand'. In effect the difference is typically a configuration setting, which in some cases may be changeable by the user. In particular most cellular smart phones contain 'airplane' mode settings that disable all internal radios allowing a user authenticated to the device operating system via password or personal identification number (PIN) to disable the cellular system. Access to this functionality may be disabled through the use of some MDM systems which would necessitate a complete power down of the device while carried on aircraft. Additionally, someone illicitly obtaining a device with properly configured password requirements and screen lock timeouts would be unlikely to guess the device password before the device was reported stolen in order for them to disable the cellular connection and prevent tracking or a remote wipe of the device.

Cellular networks do not allow for the same level of exposure of individual devices to random access from the internet. This significantly reduces the potential network based attack vectors that might reach a cellular connected device. The risk scenario in most cases from a network based attack would be similar to a device protected behind rudimentary network defenses (e.g. standard firewall but NOT advanced intrusion detection/prevention) Cellular device communications cannot typically be accessed by other 'eavesdropping' devices physically close to them without significant specialized equipment and can be considered well protected against network attacks below the nation/state level of technical capability by the hosting technical infrastructure and technology inherent in the device. However, network based attacks that utilize connections initiated by the user device may still succeed over the cellular infrastructure. For this reason, the technical protections inherent in the cellular infrastructure provide limited protection against user/device initiated actions (e.g. web surfing on a cellular connected web browser). Therefore, the protections provided by always on cellular connections are primarily in the ability to remotely access the mobile device for tracking or data deletion in case of device loss or compromise, which combined with a limited functionality device operating system, the protections are generally equivalent to a 'personal firewall' if properly configured and supported by a well-designed organizational infrastructure. However, that equivalency does not apply to full featured operating systems connected through cellular infrastructure.

NOTE: It should be noted that a technically capable, intentional, thief knowingly obtaining an 'always on' cellular device for the purpose of data theft can physically disable the radio by utilizing a Faraday cage or similar external electromagnetic shield device while attempting to guess the device password. While technically possible these methods require specialized equipment and high technical expertise and would be very unlikely to be employed except for specifically targeted attacks. When always on cellular connectivity is combined with a robust incident reporting process and user training for rapid response to device loss or theft, the associated risks can be minimized.

WiFi only (includes 'on-demand' cellular)

WiFi only devices do not include cellular radios or include cellular radio that must be manually activated or 'connected' to the cellular network. They connect to the network or internet through WiFi 'hotspots' or external access points or manually to cellular networks. Some MDM or device configurations may be able to limit the types and specific WiFi access points the device can connect to, which may change the risk scenario of the device to a similar risk scenario as the Cellular Network Only scenario. However, if mobile devices are permitted (through technical and or policy decisions) to connect to any WiFi access point designated by the device user, the overall device risk scenario is high and the device may be accessible to a large number of potential network based attack vectors. Unrestricted WiFi access is not recommended on any agency owned device, but must be assumed to exist on any personally owned device authorized to access CJI. Significant compensating controls may be needed to ensure devices accessing CJI over 'public' WiFi access points are not susceptible to communications network eavesdropping, credential hijacking or any of the various potential man-in-the-middle attacks possible through access point spoofing. The communications security risks can be significantly mitigated by mandatory device configurations (e.g. MDM based policy) that only allow devices to connect to cryptographically verified agency controlled WiFi access points.

WiFi only or devices with 'on-demand' cellular access (e.g. user or event driven cellular access initiated from the device and not from a centralized management location) are significantly more at risk from data loss subsequent to device loss or theft as there is no guarantee the tracking or remote wipe can be initiated once the device is out of agency control. This can be mitigated by utilizing tracking/anti-theft products that require a periodic network connection to authorize access and perform automated device locking ('bricking') or remote wipe if network connections are not made within a specified period. Software of this nature is generally available for full featured laptops but may not be available for limited feature mobile operating systems.

Cellular (always on) + WiFi Network

This is a hybrid scenario that has become typical with most 'smartphones'. These devices contain both the always on cellular connection, but may also be configured to access local WiFi networks for enhanced bandwidth. In considering devices with these technical characteristics, the theft/loss risks are similar to the cellular only scenario (due to tracking and remote access through the cellular connection), while the data and network based risks must be considered to be similar to the WiFi scenario unless the capability of the device to connect to WiFi networks is limited by technology or policy to agency owned WiFi Access Points configured in accordance with the CJIS Security Policy. Careful consideration must be made to the particular configurations, management systems, and human oriented operational policies based on the particular technical capabilities and configurations of these types of devices.

Incident Handling (CJIS Security Policy Section 5.3)

Additional or enhanced incident reporting and handling procedures will need to be developed to cover mobile device operating scenarios. Various exploits and methods to compromise mobile devices require either specialized equipment or lengthy operations to implement. Rapid response to mobile device related incidents can significantly mitigate the risks associated with illicit data access either on the device itself or within online data resources associated with the device through an application or specialized interface. However, parallel or special incident handling procedures with associated equipment or systems may need to be put in place to properly respond to incidents involving mobile devices. This section lists three areas where enhanced incident handling and

response processes may need to be implemented to ensure mobile device compliance to the incident handling policy in Section 5.3.

If personally owned devices are utilized within the environment in a Bring Your Own device (BYOD) scenario, specialized and costly incident handling procedures and processes may need to be developed to support compliance for those devices. The costs associated with enhanced incident handling procedures may need to be incorporated in the cost and risk based analysis to allow personally owned devices in the BYOD scenario, as the technical methods and risk to achieve compliance under BYOD scenarios may exceed any cost savings potentially achieved through BYOD.

Loss of device Control

Mobile device users should be trained and provided with explicit user actions in case positive control of a mobile device is lost for any period of time. Loss of positive control means the device is in the physical control of non-CJIS authorized individual or the device is left unattended in an unsecure location (e.g. counter of the coffee shop). Even if the device is recovered quickly there is significant risk that either the device settings could be tampered with or data on the device could be illicitly accessed. The level of detail and particular scenarios identified in the agency incident response plan should be consistent with the presence of persistent CJI on the device or the technical means used to access CJI from the device (e.g. ask the question: "Is it reasonable to assume CJI could be accessed") as well as the degree of device configuration control exercised by the user from the device main login. At a minimum, special incident handling procedures should be developed for the following scenarios:

- Device known to be locked, control loss of minimal duration
- Device lock state unknown at time of control loss, duration of loss minimal
- Device lock state unknown at time of control loss, duration of loss extended
- Device known to be unlocked at time of control loss, duration of loss more than momentary.

NOTE: Organizations should define appropriate time value criteria based on the operational environment for the above scenarios. For instance, a 'momentary' loss of control might be considered a matter of seconds in a situation where no one could reasonably have accessed the device, while 'minimal' durations might include a few minutes of time and 'extended' periods would be any time longer than a few minutes.

Other scenarios should be addressed as appropriate to the intended device employment, with explicit user and organizational actions identified based on the device technologies and any organizational management capabilities.

Total Loss of device

Incident response scenarios for the total loss of the device should be developed based on the methods/storage of CJI on the device, the lock state of the device at time of loss (known locked, known unlocked, or unknown), and the technical methods available for remote tracking or wiping of the device. It is critical to implement incident handling procedures quickly in this case. Remote wipe functions can be implemented for always on cellular devices with a high potential for success that may include positive confirmation from the device that the wipe was completed. However, for WiFi only and on demand cellular devices, incident handling procedures that lock the device out

of accessing CJI may be necessary, while there would be no guarantee that any CJI stored on the device could not eventually be accessed. For this reason, CJI should not generally be stored directly on WiFi only or on-demand cellular devices unless an extremely robust anti-tamper system is in place on the device itself.

Potential device Compromise (software/application)

Incident response scenarios for potential device compromise through intentional or unintentional user action should be developed to ensure compliance with policy. This includes rooting, jailbreaking or malicious application installation on the device during a loss of device control scenario or inappropriate user action in the installation of applications to the device (compromise can occur from either intentional threat agent actions or accidental user actions). Triggers for this incident handling process may be driven from either user notification or electronic detection of device tampering from an audit or MDM compliance check.

Audit and Accountability (CJIS Security Policy Section 5.4)

The ability to implement some Audit and Accountability functions specified in the CJIS Security Policy on mobile devices with limited function operating systems (e.g. Android, Apple iOS) is not natively included within the operating system. Either additional device management systems, enterprise mobility management (EMM) or MDM, or auditing from systems accessed by the mobile device will be necessary to ensure appropriate levels of auditing exist.

Auditable Events (reference 5.4.1)

Some of the specific audit requirements in the CJIS Security Policy may not be technically relevant to the mobile operating system due to its internal functioning. To achieve compliance with the CJIS Security Policy it will be necessary in most cases to utilize some form of MDM or EMM system. Additional auditable events that compensate for the technical limitations of limited function mobile operating systems may be available through the use of MDM systems (e.g. association of event with global positioning system (GPS) location of the device). Specific auditable events of interest in the mobile environment will depend on the intended device usage, compartmentalization of data on the device, and options available with the specific technologies employed. For instance, item 2 in Section 5.4.1.1 indicates an auditable event includes attempts to modify elements of user account modification. Due to the limited internal functions of mobile operating systems, this event type is not relevant to the operating system itself as they are generally provisioned with only a single non-modifiable user account on the device. To achieve compliance in a scenario where CJI is stored or accessed from a secure application on the device, auditing of access to the secure application either through application design, or third party MDM capability may provide an acceptable compensating control. For compliance with the policy each auditable event and event content must be compared to the particular technologies and applications employed to determine if adequate compensating controls are being met for audit items that either do not apply to mobile technologies or cannot be implemented within the technology itself.

Alternative and compensating controls that provide detailed audit of access to CJI either on the mobile device itself or through a controlled application to a central server may provide equivalent auditing capability to the events specified in the policy. However, multiple auditing systems may be required to replicate the auditing provided at the operating system level by a full function operating system. Therefore, the overall auditing design should take into account retrieval and

consolidation of events or audit data from multiple auditing systems as appropriate to comply with policy.

Audit Event Collection

Mobile devices without an 'always-on' cellular connection may pose technical challenges to ensure any audit records collected and stored on the mobile device itself can be retrieved for review and analysis per the CJIS Security Policy. Alternatively systems which explicitly require a network connection to a central server to access data or decrypt on-device storage may provide acceptable audit event collection and reporting since there is a guarantee that network connections must be in place for CJI to be accessed. Careful consideration should be made regarding the accessibility of audit records when developing the mobile audit scheme.

Access Control (CJIS Policy Section 5.5)

Access control associated to limited functionality mobile operating systems will typically operate in a different manner than full function operating systems. For instance there is normally not a provision for multiple user accounts on many mobile operating systems which may mean the policy requirements for access control (e.g. regarding account management) would not be apply to the mobile operating system, but should rather be applied to a particular application, either stand-alone to the device or as part of a client server architecture. Application of access control policy identified in the CJIS Security Policy will often need to be applied to elements of the total system beyond the device operating system.

For example, CJI stored or accessed from a secure mobile application that requires connectivity to a CJIS authorized server architecture could potentially accomplish most or all of the access control policy elements based on user authorization via the secured application and be largely independent of the mobile operating system. Alternatively, if storing CJI in 'general' purpose data storage containers on a mobile device it may not be possible to achieve compliance with the CJIS Security Policy. Careful consideration and deliberate design of mobile applications or data storage will be required to achieve compliance on mobile devices.

Due to the inherent nature of limited function mobile operating systems, very tight access controls to specific data is actually implemented within the operating system. This effectively prevents applications from accessing or manipulating data associated with other applications to a very high degree of confidence as long as the device is not rooted or jailbroken. However, the device user is automatically granted access to all device data through the associated application unless the application itself has a secondary authentication and access control methodology. Additionally, since basic device functions (e.g. phone) are typically protected using the same password or PIN as the device level encryption, use of a weak PIN to allow easy access to basic device functions largely negates the value of the integrated device encryption.

If personally owned devices are utilized within the environment (BYOD scenario), specialized and costly access control methods may be required to reach compliance with CJIS Security Policy. The costs associated with enhanced access control procedures and technologies should be incorporated in the cost and risk based analysis to determine whether or not to allow personally BYOD, as the technical methods and compensating controls required for CJIS Security Policy compliance are likely to exceed any potential cost savings for implementing BYOD.

Device Control levels and access.

Limited function mobile operating systems are typically very constrained on the levels of access provided to the user. However, intentional user actions (e.g. installing an application and accepting inappropriate security access levels for that application) may bypass some of the built in security protections inherent in the limited functionality devices. Compliance with CJIS Security Policy may be difficult without the addition of strict device control policy. In a mixed environment (e.g. agency owned devices and BYOD), access control policy with BYOD systems may be impractical or impossible to fully implement.

Embedded passwords/login tied to device PIN.

Limited function mobile operating systems typically allow the association of multiple passwords and access credentials with particular applications. The system access provided by these embedded credentials will often be tied to the device password or PIN. An example would be access to device integrated email and calendar applications. Alternatively a 'corporate' email application may independently encrypt the data associated with the application and require a separate login from the device itself. Access to CJI utilizing only the device level password or PIN and device embedded credentials is not compliant with CJIS Security Policy unless protected with Advanced Authentication, which is not currently possible on most devices. Therefore, use of integrated device functions (e.g. built in email or chat) to store or transmit CJI would also not be compliant.

Access requirement specification

In general, due to weaknesses associated with password guessing based on analysis of fingerprints or swipes on the device touch screen, short (4-8 digit) device PIN numbers provide limited security to a determined password guessing attack. Conversely, utilization of a robust password at the device level may be inconsistent with quick access to basic device functions (e.g. phone). When developing specific CJIS compliant access control and authentication schemas a layered approach with the device PIN protecting only the basic device functions (e.g. phone, camera, non-secure applications) and a more robust password or multifactor authentication used to protect applications or data storage may achieve policy compliance where the device password/PIN would not. In a layered security deployment, careful attention must be placed on the capability to share data (e.g. cut and paste or screenshot functions) between secure applications with CJI or CJI access and basic device functions with limited security controls.

Special Login attempt limit

Depending on the access and authentication scheme applied to the mobile device, it may be appropriate to fully comply with the CJIS login attempt limits within a secure application or container and not solely at the device level. However, the device itself should have login attempt limits consistent with the risk associated to the data or configurations accessible on the device itself. Since mobile devices are inherently portable, and can easily be removed from a location. Brute force attempts to gain access to the system, especially when protected only by a short PIN, are likely to be successful given sufficient time. Special consideration should be made based on device connectivity methods (cellular, WiFi, etc) on the appropriate number of unsuccessful login attempts that will be allowed and the resultant actions taken by the device. Most devices either natively allow for the device to wipe itself after a failed number of attempts, or allow the application of EMM/MDM applications to perform wiping actions after a predetermined number of failed login attempts.

Login failure actions

Mobile devices with or without MDM software can typically be configured to perform actions based on serial unsuccessful login attempts. Appropriate actions to configure may be dependent on the data resident on the device and the connectivity method employed by the device. Most devices can be configured to delete all data on the device and/or issue an alert to the network if a number of incorrect passwords are entered. This is a very advantageous feature, however specific configuration of the number of attempts and resultant action must be considered against the state of the device after an unsuccessful attempt action is triggered. A full device wipe will typically leave the device in a fully or partially non-functional state which could introduce risk if part of the intended use is time critical phone calls. Where possible, full device wipe associated with unsuccessful attempts at the device level password should be configured but the number of invalid attempts may exceed the CJIS Security Policy at the device level if all CJI on the device is protected by an additional layer of encryption protected by a subsequent secure application authentication method that is technically prevented (via complexity rules or entry rules) from being the same as the device level authentication and the secure application is configured in accordance with the policy and also contains a secure data wipe capability after a specified number of incorrect authentication attempts.

System use Notification (CJIS Policy reference 5.5.4)

Agency policy should include specific mandatory language consistent with the CJIS Security Policy to identify the device restrictions and consent. However, due to screen size limits, some mobile devices may not be technically capable of displaying the full text used with traditional operating systems. To achieve compliance agencies should contact their legal department for appropriate wording of a short version of the system use notification that can be set to display within the constraints of the device lock screen. This may be accomplished through embedding the text into an image displayed on the lock screen or some other external device labeling method if the device does not permit sufficient text to be displayed.

In a BYOD environment or mixed (agency owned and BYOD), it may be necessary to develop or deploy custom applications that can achieve compliance with the system use notification upon access and prior to any CJI access being allowed.

Session Lock (CJIS Policy reference 5.5.5)

Due to the portable nature of mobile devices the session lock limit in the general CJIS Security Policy may be excessive in the mobile environment for certain device functions and insufficient for other functions based on intended device usage. Agencies should examine the minimum lock time practical for all mobile devices based on their employment scenario and ease for which a user can manually lock the device. The actual session lock times should be adjusted as appropriate to the device type, device operational location, and the data accessible on the device when unlocked. Pocket size devices are at greatest risk if screen lock times are insufficient, however, for devices used in emergency response or communication, extended lock times at the basic device level may be considered if CJI is subsequently protected by an application or web interface utilizing more stringent secure locking functions. A well designed solution may include multiple session lock settings at the device and individual application levels to ensure the CJIS Security Policy requirements are met for CJI access, while other device functions are accessible under different session lock configurations.

Device WiFi Policy

Specific WiFi configuration policy should be developed based on the intended use environment and data access requirements for the device. The policy should explicitly cover configuration of device connections. Technical methods specific to the mobile technologies may need to be implemented to ensure all mobile devices are compliant with CJIS Security Policy. Current CJIS Security Policy provides detailed configuration requirements for WiFi connections, however it was originally intended for defining requirements for fixed infrastructure WiFi (802.11) supporting wireless within a facility. The security requirements identified for fixed infrastructure installations are applicable to mobile usage, however there are several mobile specific scenarios where the requirements may not be clear. The following sections identify areas not specifically covered in the existing policy that will require special handling to ensure wireless connections are compliant.

Hotspot capability

Many mobile devices now include the capability to activate an internal WiFi hotspot that allows other devices to connect through the hosting device to the internet over the devices cellular radio. While this is a potentially valuable capability when multiple law enforcement devices may need localized internet or network access, mobile hotspots should be configured as consistent with the CJIS Security Policy on wireless access points. Connections must only be accepted from known and approved devices in order to protect the integrity of the hosting device as well as the communications security of other connected devices. Since most mobile hotspots are not technically capable of providing the device authentication required for infrastructure wireless, use of mobile hotspot capability should assume the overall portable WiFi network itself is not secure and CJI should not be transmitted or exposed on the network without appropriate encryption.

Connection to public hotspots

There are significant risks to connecting to public wireless access points. Rogue access points masquerading as legitimate public access points may allow for man-in-the-middle, eavesdropping, and session hijacking attacks. While not specifically prohibited in the current CJIS Security Policy, it is recommended that connection to public internet access points be technically restricted by device configuration or MDM systems if possible. CJI access mechanisms from mobile devices should include robust authentication methods specifically designed to prevent interception or hijacking of CJI or user information through the use of a rogue access point masquerading as a legitimate public wireless access point. Transmission encryption alone may not provide sufficient protections when device connections originate at public hotspots. Since the public hotspot controls access to all network services at the connection point (e.g. Domain Name System) attacks against the transmission path are possible that would not normally be feasible in a fixed environment where communications exist between two secured network enclaves.

Cellular Service abroad

If mobile devices are used outside of the United States, especially if connected to foreign cellular networks, specific handling procedures may need to be developed for the use of the device while abroad and the assessment or configuration check of the device state once the devices are returned to the United States. Certain device internal functions on cellular devices may be modified or compromised by the cellular carrier as the devices are intended to have certain parameters configured by the cellular service provider which is considered a 'trusted' entity by the device.

Cellular carriers within the United States are constrained by United States laws regarding acceptable modifications to devices. Similar legal constraints cannot be assumed to exist in some areas of the world where laws and regulations for data and personal privacy may allow cellular carriers significantly more leeway in changes made to devices on their networks.

Security plans involving cellular connected devices that will be connected to foreign cellular networks should include technical and policy controls to ensure device use while abroad, data resident on the device while abroad, and the software integrity of the device once returned to the United States are all appropriate to the specific device and threat levels associated with the expected foreign travel. This should explicitly include considerations for devices in which an internal subscriber identity module (SIM) card is inserted into the device to obtain Global System for Mobile (GSM) cellular connections abroad to ensure any residual data on the SIM card is properly purged. Additionally, incident handling procedures may need to specify more stringent responses to even momentary loss of device control, and it may not be possible to assume tracking, anti-theft, and remote data wipe functions that work in the United States would be functional in all potentially visited geographic and political regions.

Bluetooth

Mobile devices utilizing Bluetooth should be evaluated for their ability to comply with the CJIS Security Policy Bluetooth requirements prior to acquisition. This includes the data device itself and any authorized Bluetooth accessories which will be associated to the device. While the technical security in current versions of Bluetooth is significantly stronger than legacy versions, mis-configuration of devices can still pose a significant threat in the mobile environment. If not specifically utilized for a required purpose, it would likely be most cost effective to disable or restrict the device Bluetooth radio utilizing device configurations or an MDM product. Additionally, the using agency may need to develop technically extensive training or user awareness programs to ensure use of Bluetooth capability does not render the device out of compliance if device users have the ability to make Bluetooth associations to the device. Specific instructions or guidance for specific devices could be developed to ensure all implementations are compliant.

Voice/Voice over IP (VoIP)

Cellular voice transmissions are distinctly different at the technical level than Voice over IP (VoIP) transmissions using voice/video applications (e.g. FaceTime, Skype). The use of VoIP is not specifically granted the exemption identified in CJIS Security Policy Section 5.5.7.3.2. Agencies wishing to use capability of this type should ensure the specific technical implementation complies with the Policy on authentication and data encryption.

Chat/Text

Device integrated chat/texting applications and many common third party chat applications authenticate and are identified using embedded passwords or the device identifier only. These functions should not be considered secure or appropriate for transmission of CJI data. Texting functions that utilize a cellular service providers Short Message Service (SMS) or Multimedia Messaging Services (MMS) functions do not constitute a secure transmission medium. Third party applications utilizing appropriate encryption and authentication methods independent of the device password/PIN may provide a compliant solution where the device integrated utilities are will not provide a compliant solution.

Administrative Access

Local administrative access to the mobile device, regardless of device category should be restricted by some mechanism. For traditional operating systems, configuration of a separate administrative account other than that used for normal logins to the device is an acceptable method to ensure appropriate access permissions to the mobile user for which they are authorized. However for limited functionality mobile operating systems (e.g. Android, Apple iOS) internal permissions and accounts assume a single authorized device user with explicitly defined permissions. Those permissions may be modified through policy applied to the device, but are typically global to the device itself. As a result, to ensure appropriate separation of access permissions, it may be required to ensure specific applications or software on the device are configured with individual authentication methods to separate application data from 'general user' access. Without additional authentication at the application level, access to specific application data would be available to any user with the ability to unlock the device. This may be appropriate in some scenarios with a high degree of assurance that the device can only be accessed by a single user, but sufficiently stringent device passwords and short screen lock times may prove problematic for practical use of some device functions. An alternate method to ensure strict separation of 'routine' device functions which may be accessed by multiple individuals (e.g. phone function if loaned to someone for a critical call) is to ensure any method used to access or store CJI has a separate and more stringent authentication method configured with rules that make it impossible to use the same authentication credential (e.g. PIN/Password) on both the device authentication and the application or function with access to CJI.

Rooting/Jailbreaking

'Rooting' (Android OS) or 'Jailbreaking' (Apple iOS) refer to intentional modifications to the mobile device operating system in order to grant the device user or an installed application elevated control that would not normally exist on the device. The security model internal to the various mobile device architectures vary significantly, however the common effect of rooting or jailbreaking the devices is to bypass many or all of the built in security features. The security feature bypass may be universal to all device features and installed applications once completed. Intentionally rooting or jailbreaking mobile devices should be avoided in any scenario as it potentially defeats all built-in data access and segregation controls on the device. Additionally the rooting or jailbreaking process itself has a heightened risk of introducing malicious code as part of the process, and also substantially increases the risk for malware to infect the device through user action. Extreme caution should be used if software is being installed that requires the devices to be rooted or jailbroken for the software or application to function. This is inclusive of purported security software that requires a rooted or jailbroken device to function. For example, on both the Android and Apple iOS platforms, the built-in security features for data access and memory segmentation prevent the effective operation of 'traditional' anti-virus and intrusion detection/prevention software. Software or applications purporting to perform these functions but requiring rooting or jailbreaking of the device and may actually accomplish the anti-virus or IDS/IPS function but are also likely to significantly increase the overall risk associated to the device by effectively disabling most or all of the integrated security features. A careful risk-based assessment should be conducted by a trained security professional prior to allowing the operation of any rooted or jailbroken mobile devices regardless of intended use. Significant compensating controls would be required to return a rooted or jailbroken device to minimal compliance with most of the CJIS Security Policy and would likely not be a cost effective approach.

NOTE: There is a distinction between rooting a 'stock' Android installation vice the installation of a separately supported secure operating system. There are secure versions of Android available or that can be developed based on the open source Android source code and compiled for installation on a particular hardware device. Installation of a secure, supported mobile operating system that replaces the device original operating system may significantly enhance the security of the device and should not be confused with 'rooting' and Android installation. Due to the close integration of operating system security with hardware elements, and the proprietary nature of Apple source code, there are not currently separate 'secure' versions of the Apple iOS and it is unlikely they will be developed.

Identity and Authentication

Due to the technical methods used for identity and authentication on many limited functionality mobile operating systems, achieving compliance to CJIS Security Policy may require layering of identification and authentication mechanisms. With the complexity and large number of potential identity and authentication solutions in the mobile environment emphasis must be placed on designing secure identity management and authentication architecture prior to the selection of individual devices or applications. Failure to consider a robust identity and authentication scheme as part of system design or acquisition will significantly increase the risk of subsequent noncompliance with CJIS Security Policy and potential added costs for a remedial solution. Many identity and authentication schemes used by existing commercial applications may make claims that appear to be consistent with CJIS Security Policy Advanced Authentication requirements, however, extreme care must be taken to ensure the actual technical implementation is compliant with policy.

Utilizing Unique device Identification

Some commercial applications and features integrated with some mobile operating systems permit the mobile device to be uniquely identified in a cryptographically robust manner. Any authentication schema that considers the possession of the mobile device as a factor in uniquely identifying and authenticating a CJIS authorized user must also include factors beyond than mere possession of the device. Larger form factor devices that cannot be carried on the person of the authorized user should not rely on possession of the device as an identifying factor, but may still include identifying capability within the device to provide assurance that the device itself is an authorized device. This should still be coupled with multi-factor advanced authentication to the device itself or the application hosting CJI. Coupling unique device authentication with robust advanced authentication of the user provides a high degree of confidence that both the specific device and the operator of the device are correctly identified. Utilizing device unique identification in order to authorize initial connections from the remote device back to the CJI hosting system or enclave provides additional protection to the CJI hosting system to reduce the attack surface of the hosting system and should be considered a good practice, but not in itself an authentication mechanism for the device user.

Certificate Use

One method for uniquely identifying mobile devices is to place part of a public key pair on the device in the form of a public key certificate. While there is value to ensuring the device itself can authenticate to a system supplying CJI, and may provide a critical layer of identification or authentication in a larger scheme, a certificate alone placed on the device should not be considered valid proof that the device is being operated by an authorized CJIS user, only that the device itself is authorized to host CJIS users. Additional user identification and authentication should be used to supplement any device certificate installed. Using a PIN or password separate from the device login to 'unlock' the certificate from cryptographic storage within a secure application will provide an additional layer of security and may increase the confidence level the device is being used by the intended user. However, use of public/private key pairs or pre-shared encryption keys can be utilized as part of an architecture to protect against certain session hijacking or man-in-the-middle attacks a mobile device may be susceptible to if connected to public internet connections.

Certificate Protections

Any certificates or cryptographic keys stored on any mobile device should include protections against the certificate or key being extracted from the device. Additionally certificates or other keys stored on mobile devices that grant the device special access or unique identification should be configured for remote wipe on demand or self-deletion based on a number of unsuccessful login or access attempts. Alternatively, methods may be used to revoke or invalidate the unique certificate or keys associated with a device.

Minimum Password/Pin (Reference CJIS Security Policy Section 5.6.2.1)

The minimum password protections identified in the CJIS Security Policy may not be appropriate for the device PIN/password due to immediate access requirement for some device functions (e.g. phone function) secured by the device PIN/password and the difficulty to enter a complex password under emergency conditions on a small screen. In cases where the risk of a complex password on the device itself is deemed significant, a layered authentication approach may be necessary where CJI or access to CJI is protected via one or more additional layers of access control beyond the device PIN/password. In cases where the CJI or access to the CJI is cryptographically segregated from applications accessible using the device level PIN/Password (e.g. secure application or secure browser vice the built-in browser) the authentication mechanism for the secure application or browser may satisfy the CJIS Security Policy requirements if fully compliant as a stand-alone application.

Configuration Management

Due to the potential for inconsistent network access or monitoring capability on mobile devices, methods used to monitor and manage the configuration of traditional full featured operating systems may not function properly on limited function mobile operating systems. Configuration Management systems in the mobile environment may be designed in order to duplicate some of the functions typically performed by traditional anti-malware systems that will not function properly on some mobile operating systems.

Mobile Device Management (MDM)/Enterprise Mobility Management (EMM)

MDM and EMM systems and applications coupled with device specific technical policy can provide a robust method for device configuration management if properly implemented. MDM capabilities include the application of mandatory policy settings on the device, detection of

unauthorized configurations or software/applications, detection of rooting/jailbreaking of the device, and many other security policy related functions. In many cases, the most cost effective way to achieve CJIS Security Policy compliance on mobile devices is the selection of MDM or EMM applications and infrastructure appropriate to the mobile operating systems and intended access to CJI on the mobile devices. MDM/EMM functions may be applicable to most of the CJIS Security Policy requirements and allow for significant compensating controls in areas where traditional methods of CJIS Security Policy compliance are not technically feasible. Section 5.5.7.3.3 of the CJIS Security Policy specifies the minimum functions required for MDM. However, careful selection of the MDM product will potentially provide a cost effective method for additional areas of compliance in the access, auditing, incident response, authentication, media protection and system integrity sections of the CJIS Security Policy.

Device Backups/Images

Device images and backups provide protection against data loss, but also provide a method to quickly recover a device after damage or potential compromise. Due to an inherently limited ability to access the internal file structure of mobile devices, it can be difficult to easily identify a device compromise or illicit modification of the device. Some device imaging and assessment software may provide a secondary forensic capability, especially if there is intent for the device to be used outside the United States.

Bring Your Own device (BYOD) employment

BYOD environments pose significant challenges to the management of secure device configurations. In many cases it may be impossible to apply effective security that is acceptable to the device owner or it may require extremely costly compensating controls to allow access to CJI on personally owned devices. While allowed by the CJIS Security Policy, agencies are advised to conduct a detailed cost analysis of the ancillary costs of compliance with CJIS Security Policy on personally owned devices when they are approved for use. In some cases, a BYOD user may agree to abide by the same device configurations and limitations as imposed on an agency owned device, but signed user agreements should still be in place to ensure the agency has a legal right to recover or clear the device of all data prior to device disposal or employee termination. In other cases, robust secure applications may provide acceptable levels of compliance in a BYOD environment for limited CJI access but application design and architecture should assume the device itself is un-trusted. If MDM/EMM software capable of detecting rooting or jailbreaking of the device is not installed, any CJIS or data access occurring from the device is at a substantially higher risk of compromise.

Configurations and tests

Common configurations specific to all employed mobile devices should be developed to ensure compliance. Configuration tests should be developed and executed on all versions of mobile devices under all possible connectivity scenarios to ensure CJIS Security Policy compliance under all expected operating conditions. Since mobile devices can expect to operate in different physical and network environments, testing and validating correct security functions is more critical than on fixed computing platforms. Additionally, security functions that function properly on one version of a mobile operating system on a particular device may not function in the same manner even on the same version on a different device or a different version on the same device.

Media Protection

Some mobile device hardware platforms include the ability to add removable storage in the form of memory cards. This function is primarily related to Android and Windows mobile platforms and is intentionally limited on Apple devices, but may be possible through certain application functions. While the Android platform performs robust cryptographic separation of data stores between applications within the 'internal' storage of the device, the Android OS does not provide secure separation of data stores on 'external' storage. Some Android hardware devices include additional storage hardwired inside the device that is classified by the operating system as external storage and the normal separation between applications accessing that storage is not applied. Each potential device considered for acquisition must be assessed regarding specific 'external' media protection requirements which may actually include built-in media or storage.

Protection of device connected media

As a result of the limited protection and encryption capabilities applied to device removable media and SIM cards for cellular provisioning that include onboard data storage, all externally removable media or memory should be handled consistently with the CJIS Security Policy on media protection.

Encryption for device media

While most mobile operating systems have the capability to encrypt internal storage, it may require specific device settings to be enabled. All mobile device storage should meet the encryption requirements identified for media in the CJIS Security Policy. Specific settings may need to be applied to ensure proper encryption is actually employed. Additionally, the device built-in encryption capability is typically tied to the device PIN or password. Depending on the device PIN or password requirements the integrated encryption may be easily bypassed by password guessing and appropriate consideration should be made to ensure additional encryption protected by advanced authentication methods be applied to all CJI.

Physical Protection

Due to small form factors and the fact that mobile devices are often stored in lower security areas and vehicles, physical protection of the devices must be considered in both policy and training. Physical protections will often be the responsibility of the assigned device user and physical protections typically inherited by individual information systems from a secure facility will not be available to mobile devices which will require compensating controls to achieve compliance.

Device Tracking/Recovery

MDM software as well as some integrated mobile operating system functions may allow tracking of stolen or lost devices via 'always-on' cellular data connections and the devices built-in GPS. Device tracking with WiFi only or 'on-demand' cellular access may not be reliable. Enabling device tracking capabilities, while not a replacement for secure storage, could be a compensating control used to substantially reduce overall device risk in some scenarios. Device tracking is not currently required in the CJIS Security Policy but should be applied to agency owned devices where possible as a risk mitigation factor. Enabling of device tracking on personally owned devices in a BYOD environment may raise employee privacy concerns and should be considered only for critical systems with the full knowledge of the employee and concurrence of the legal department. This is an enhanced risk that must be accepted for BYOD employments and should be considered

when allowing BYOD employment. Device tracking is available for both limited function mobile operating systems as well as traditional operating systems installed on laptop devices.

Access to device tracking software or applications within the organization should be controlled with limits and formal processes required to initiate a tracking action. It is advisable to include appropriate clauses in user agreements under what conditions and controls the organization applies to device tracking.

Devices utilizing unique device identification/certificates

Devices utilizing unique device identification or have installed certificates may require additional physical protection and/or additional incident handling steps in case of device loss in order to ensure the device unique identifier or certificate is immediately revoked or disabled. Additional physical protection rules or policy would be appropriate for any device which contains access mechanisms tied to the device.

System Integrity (CJIS Policy Section 5.10)

Managing system integrity on limited function mobile operating systems may require methods and technologies significantly different from traditional full feature operating systems. In many cases the requirements of Section 5.10 of the CJIS Security Policy cannot be met with a mobile device without the installation of a third party MDM or EMM application and supporting server infrastructure.

Patching/Updates

MDM software may provide compliance to the Section 5.10.4.1 patch management requirements for particular platforms and software versions. However, devices without 'always-on' cellular connections may not be reachable for extended periods of time by the MDM or EMM solution either to report status or initiate patching. Supplementary or manual device accountability methods may need to be implemented to account for devices without persistent connections to ensure their patch and update state is current. Alternatively, some patches or system updates may not be practical over cellular connections and will require connection of devices to a WiFi network. Compliance with CJIS Security Policy requirements through purely technical means may not be practical and considerations should be made for aggressive management of devices through training and mandatory periodic connection of devices to organizationally managed WiFi networks.

TECHNOLOGY NOTE: Apple and Android based devices have different potential issues regarding device operating system updates. Apple maintains support for updating the operating system on Apple hardware for several device generations (typically 3-5 years) and provides a robust mechanism for system updates. However, updates to Android based systems are driven by the individual device manufacturer which may or may not support regular updates to current Android operating system versions. Additionally, different Android device vendors may offer updates/upgrades to the Android operating system on different schedules, which can complicate environments utilizing Android devices from multiple manufacturers.

Malicious code protection/Restriction of installed applications and application permissions

MDM or EMM software will typically allow restrictions on installed applications. One of the few effective attack vectors to compromise mobile operating systems is to manipulate the device user to install a malicious application. Even though the application may be restricted from accessing

other application data, it may have some access to common data stores on the device and access to device functions (e.g. GPS, microphone, and camera) that are undesirable. Unrestricted installation of applications by the device user could pose a significant risk to the device.

Malicious code protection using traditional virus scanning software is technically infeasible on most limited function mobile operating systems that are not rooted or jailbroken. The integrated data and program separations prevent any third party installed program from accessing or 'scanning' within another application data container. Even if feasible, power and storage limitations would be prohibitive in the effect on device battery life and storage capacity on most mobile devices. However, the cryptographic separation between applications and effective application virtualization technologies built into common mobile operating systems partially compensate for the lack of traditional virus scanning technologies. Appropriately configured MDM software is capable of checking the installed applications on the device and reporting the software inventory to a central management console in a manner analogous to traditional virus scan detection of unauthorized software. This behavior is analogous to the software inventory performed by anti-virus products and can provide a high degree of confidence that only known software or applications are installed on the device. While it is theoretically possible to bypass the application sandboxing and data segregation protections to compromise a mobile device through the web browser, the attack methods required are significantly more advanced than those required for a traditional full featured operating system. Malicious code protections on the device web browser can be enforced through the use of a properly protected web proxy which the device is configured to use as a mandatory device policy. The most common method of malicious code installation is enticing the user to manually install the malicious app which can be mitigated on organizational devices using an MDM or other application installation restrictions which prevent the user from installing unauthorized or unknown applications. Mitigation of this issue within BYOD environments may not be possible and will present a significantly enhanced risk to the device.

TECHNOLOGY NOTE: In the particular area of application installation there is a significant difference between the behavior of Apple iOS and Android platforms. Apple cryptographically restricts the way applications will execute on the device and assigns mandatory application permissions when the application code is signed prior to release on the Apple App Store for distribution. Apps on the Apple platform must conform to Apple's policy on app behavior and cannot exceed their design permissions on access to common device functions once the app has been signed and distributed. However, the Apple method does not typically advertise the precise internal permissions granted to the app to the user prior to installation. At runtime, the app is required to request user permission to access certain device functions, and the user may agree or not agree, which may introduce risk if they are unaware of what they are agreeing to allow. Unsigned or un-trusted apps are cryptographically prevented from executing on non-jailbroken iOS devices. Apple provides a mechanism for organizations to distribute custom apps within an organization with equivalent protections but all receiving devices must have a special certificate installed that will only allow official App Store and the organization custom apps to execute.

Conversely, the Android platform, while also requiring app code signing, allows for self-signed code which can be distributed by means other than an official app store and execute on any Android device. Application permissions are presented to the user once at app installation but ramifications of agreement to certain app permissions may not be obvious to a non-technical user. Permissions in the Android model require user acceptance of all app requested permissions or the app is denied

installation, which can result in unwise user acceptance of excessive permissions in order to gain functionality provided by the app.

On either platform user installation of applications can significantly change the security state of the device. Applications may be able to transmit and receive data or share device common data with other devices over the network or local WiFi or Bluetooth connection. On either platform it is highly desirable to limit allowable applications to a pre-approved pool of apps via MDM or organizational App store structures and device policy. However, the risks associated with uncontrolled app installation is several orders of magnitude greater on Android based devices.

WARNING: Rooted or jailbroken devices are modified in such a manner that the built in protections against malicious code are effectively disabled. A rooted or jailbroken device would require significant and costly compensating controls to achieve compliance.

Firewall/IDS capability

Traditional device or “personal” firewalls as identified in CJIS Security Policy Section 5.10.4.4 may not be practical on limited function mobile device operating systems but significant compensating controls are available. By default, mobile device operating systems have a limited number of system services installed and carefully controlled network access. To a certain extent the mobile operating system performs similar effective functions as a personal firewall would perform on a general purpose operating system. Potential compensating controls for the five (5) personal firewall requirements specified in Section 5.10.4.4 are listed below:

1. Manage Program Access to the Internet: On agency controlled devices with an MDM, limiting the apps installed on the device will effectively perform the same function. Since no software or apps can be installed without MDM approval a robust approval process can effectively ensure internet access is only granted to approved apps. Built-in apps and functions can also be limited on network access by the MDM.
2. Block unsolicited requests to connect to the user device: Default configurations for mobile operating system platforms typically block incoming requests. It is possible to install an app that may ‘listen’ on the network and accept connections, but the same compensating control identified in item 1 will mitigate the likelihood of that occurring.
3. Filter incoming traffic by IP address or protocol: Protocol filtering effectively occurs due to the limited function of the operating sys long as no installed application opens network access ports. The mitigations in 1 effectively compensate for this control as well.
4. Filter incoming traffic by destination ports: Same as 3.
5. Maintain an IP traffic log: This may not be technically feasible on most mobile operating system platforms as maintaining this log would require access to lower level operating system functions that are not accessible unless the device is rooted or jailbroken. However, individual Apps that communicate over the network or accept connections from the network may permit logs of IP traffic associated to that application to be stored.

Spam Protection

Spam guards installed on corporate or organizational email systems may effectively accomplish the spam protection requirements for the CJIS Security Policy on mobile devices if properly configured to block spam before delivery to the device. If no upstream spam guard is installed on the mail server the mobile devices accesses, the device may not have adequate spam protection. Additionally access to internet based email (web mail) would need to be restricted to web mail with appropriate spam and/or antivirus protections to ensure compliance.

Periodic system integrity checks

One method to compensate for the technical infeasibility of traditional anti-virus and malicious code protection is to install an MDM that performs periodic system integrity checks that validate device configuration and status against an approved baseline. Deviations may provide indicators of potential device compromise or mis-configuration.

G.5 Administrator Accounts for Least Privilege and Separation of Duties

Administrator Accounts for Least Privilege and Separation of Duties

PURPOSE:

This appendix is provided to describe industry best security practices for assigning separate administrator accounts to support the concept of Least Privilege.

ATTRIBUTION:

- SANS, "The Critical Security Controls for Effective Cyber Defense", version 5.0
- NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations", Revision 4 dated April 2013
- NIST SP 800-12, "An Introduction to Computer Security: The NIST Handbook" dated October 1995
- CNSSI-4009, "National Information Assurance (IA) Glossary", dated April 2010

DEFINITIONS:

Least Privilege – The principle that security architecture be designed to grant individual users and processes only the minimum accesses to system resources and authorizations required to perform their official duties or function.

Separation of Duties – The security principle requiring the division of roles and responsibilities so that a single individual cannot subvert a critical process or function.

SUMMARY:

The implementation of least privilege is accomplished by assigning user or process access to system resources based on operational or business needs. Thus, access is granted to only those resources required to perform assigned duties. For individuals who have multiple roles within the organization requiring varying levels privileges, this assignment of access can be challenging. Often times the agency will assign a single userid to the individual and elevate the privileges for that account based on the different roles. While it may seem logical to allow the user access to all

required resources using a single account, security vulnerabilities can be introduced into the system.

Associated with least privilege is separation of duties. This concept aids in maintaining the integrity of the system by preventing the abuse of elevated privileges for making unauthorized changes to the system. This objective essentially requires different individuals to perform separate functions with relation to (primarily) administrative duties. For instance, those with the ability to create and assign user access to system should not be able to access the audit logs that contain the evidence of the account actions.

USER ACCESS AND ACCOUNT MANAGEMENT:

Several factors influence the manner in which an agency implements and manages user access. Many times, the size of the agency and the technical expertise of the IT staff employed by the agency become primary drivers. Larger agencies with a broad base of technically savvy personnel normally have the ability to dedicate resources specifically to the administration and management of user access. This could translate to the use of multiple accounts for a single user performing duties requiring varying levels of access.

Smaller agencies with few or no technically experienced personnel will often assign single user accounts with the highest level of access required by users. Other smaller agencies may go as far as assigning every user an account with elevated privileges so there are no delays or problems requiring intervention by already overburdened system administrators. It is not uncommon for a smaller agency to outsource system administration duties.

Regardless of the size or resources of an organization, each agency should base the process for assigning access to system resources based on their operational requirements and a thorough risk assessment. To mitigate risk for accessing system resources, industry best security practices prescribe those individuals performing duties requiring elevated privileges be assigned a separate userid to be used in the performance of those duties. This account would be separate from a standard user account.

Why are some agencies unwilling to implement controls for least privilege? One common reason/perception is administrative overhead. There is a time factor for a system administrator to create user accounts and configure those accounts correctly based on the user's role. In larger agencies with many employees, this could add up to a significant impact on the system administrator(s) especially if there is a high level of turnover. Resources in some agencies may allow for a single system administrator dedicated strictly for account management. On the other end of the spectrum, in agencies with fewer employees, the impact may be more burdensome. While there are fewer user accounts to manage, a full-time system administrator for account

management may not be feasible. Those duties then become shared between a few people or added to the duties of a lone person.

Another reason may be the burden on system administrators to remember multiple userids and passwords. This could result in the user using the same password for each account or the user writing down the credentials for ease of remembrance. Additionally, an administrator could get the credentials mixed up between accounts causing an account lockout. This could then require system administrator intervention to reset or unlock the account.

Some agencies may feel that creating additional accounts reduces system resources. Depending on the size of the agency, this could be a concern. In most cases, the number of individuals that would require a secondary account would be minimal. The impact could be limited to a slight increase in disk space usage on the systems accessed by the system administrators with the separate accounts and perhaps the server housing the account information.

THREATS:

A primary goal of attackers is to gain administrative or root privileges on a network or system. Therefore, protection of credentials with that level of access is a key to preventing unauthorized access. Attackers may use many methods in attempts to gain unauthorized, privileged access to computer or network systems. There are two common techniques that take advantage of improperly managed administrative privileges.

Phishing Attacks

In this first method, consider a small organization with limited system administrative resources. Each user is assigned an account with elevated privileges that allows them to perform a myriad of duties including gaining access to critical system security resources. Because this is the only account the user has, normal non-administrative duties are also performed with administrative rights. While checking their email, the user is fooled into reading a message and opening a malicious attachment. Because the user's account has elevated privileges, malware is now installed on the system with elevated privileges. The malware could now allow the attacker to take over the system and install other malicious software such as key loggers, sniffers, or remote control applications. Other key system resources such as firewalls, routers, switches, or intrusion detection systems are now also compromised.

Password Brute Force Guessing / Cracking

The second method may not be as easy as the first and involves the guessing or cracking of passwords on the part of the attacker. Based on human nature, we tend to develop passwords that

are easy to remember and most likely contain some kind of information that is pertinent to us. Some passwords could be easily guessed with a minimal amount of social engineering or fact finding. Consider again an agency that assigns users a single account to perform all duties including those requiring elevated privileges. A user has created a password that, while meeting the requirements of the CJIS Security Policy, is comprised of easily guessed information about the user. An attacker has previously determined the userid and is now able to begin guessing the password. Upon success, the attacker will have unauthorized access to critical system resources.

MITIGATION:

The first step to implementing least privilege is to create separate user accounts for those individuals that require elevated privileges for their duties. These duties could include system or security administration, reviewing audit logs, backup administration, or configuring network devices (e.g. firewalls, routers). The passwords associated with these accounts should have a higher level of complexity than an account without elevated privileges. By disassociating the access levels required for system administration functions from an individual's "everyday use account", should a password be compromised, access would be limited to that of a user with non-elevated privileges.

Second is to implement procedures to ensure accounts with elevated privileges are used only for those duties requiring the higher level of access. This would mean disabling or blocking access to email, web browsers, and other external facing connections. While technical processes are the preferred method of preventing the misuse of accounts with elevated privileges, written policies can be used in situations where technology does not support that type of account management.

Several governance organizations recognize the importance of the security value of Least Privilege. The Payment Card Industry (PCI) includes requirements in their Data Security Standards (DSS). The National Institute of Standards and Technology (NIST) addresses the concept of Least Privilege in its Special Publication (SP) 800-53 rev. 4. While not considered a governance organization, the System Administration, Networking, and Security (SANS) Institute publishes a list of the top 20 security controls which includes "Controlled Use of Administrator Privileges" at number 12. Although the actual security controls or required implementation may slightly differ, the concept is consistent across the groups. The actual controls from NIST and SANS are included here in this appendix.

NIST CONSIDERATIONS FOR LEAST PRIVILEGE:

NIST Special Publication 800-53 rev. 4 includes controls required for all systems under the Federal Information Security Management Act. The publication specifies the guidance for Least Privilege in the control catalog under the Access Control (AC) family and specifically as AC-6. While the NIST requirements are not enforceable under the CJIS Security Policy, they were the genesis of

the Policy and do provide a sound security baseline that can be leveraged by the criminal and noncriminal justice community. AC-6 is a key control having several enhancements which, when implemented, bolster the overall security of the information system by reducing the risk of compromise through the misuse or misconfiguration of access to system resources.

AC-6 Least Privilege

Control: The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Supplemental Guidance: Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems. Related controls: AC-2, AC-3, AC-5, CM-6, CM-7, PL-2.

Control Enhancements:

(1) LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS

The organization explicitly authorizes access to [Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information].

Supplemental Guidance: Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users. Related controls: AC-17, AC-18, AC-19.

Control Enhancements:

(2) LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS

The organization requires that users of information system accounts, or roles, with access to [Assignment: organization-defined security functions or security-relevant information], use non-privileged accounts or roles, when accessing nonsecurity functions.

Supplemental Guidance: This control enhancement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account. Related control: PL-4.

(3) *LEAST PRIVILEGE | NETWORK ACCESS TO PRIVILEGED COMMANDS*

The organization authorizes network access to [Assignment: organization-defined privileged commands] only for [Assignment: organization-defined compelling operational needs] and documents the rationale for such access in the security plan for the information system.

Supplemental Guidance: Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device). Related control: AC-17.

(4) *LEAST PRIVILEGE | SEPARATE PROCESSING DOMAINS*

The information system provides separate processing domains to enable finer-grained allocation of user privileges.

Supplemental Guidance: Providing separate processing domains for finer-grained allocation of user privileges includes, for example: (i) using virtualization techniques to allow additional privileges within a virtual machine while restricting privileges to other virtual machines or to the underlying actual machine; (ii) employing hardware and/or software domain separation mechanisms; and (iii) implementing separate physical domains. Related controls: AC-4, SC-3, SC-30, SC-32.

(5) *LEAST PRIVILEGE | PRIVILEGED ACCOUNTS*

The organization restricts privileged accounts on the information system to [Assignment: organization-defined personnel or roles].

Supplemental Guidance: Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information/functions. Organizations may differentiate in the application of this control enhancement between allowed privileges for local accounts and for domain accounts provided organizations retain the ability to control information system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk. Related control: CM-6.

(6) LEAST PRIVILEGE | PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS

The organization prohibits privileged access to the information system by non-organizational users.

Supplemental Guidance: Related control: IA-8.

(7) LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES

The organization:

- (a) Reviews [Assignment: organization-defined frequency] the privileges assigned to [Assignment: organization-defined roles or classes of users] to validate the need for such privileges; and**
- (b) Reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.**

Supplemental Guidance: The need for certain assigned user privileges may change over time reflecting changes in organizational missions/business function, environments of operation, technologies, or threat. Periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions. Related control: CA-7.

(8) LEAST PRIVILEGE | PRIVILEGE LEVELS FOR CODE EXECUTION

The information system prevents [Assignment: organization-defined software] from executing at higher privilege levels than users executing the software.

Supplemental Guidance: In certain situations, software applications/programs need to execute with elevated privileges to perform required functions. However, if the privileges required for execution are at a higher level than the privileges assigned to organizational users invoking such

applications/programs, those users are indirectly provided with greater privileges than assigned by organizations.

(9) LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS

The information system audits the execution of privileged functions.

Supplemental Guidance: Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat (APT). Related control: AU-2.

(10) LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS

The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

Supplemental Guidance: Privileged functions include, for example, establishing information system accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.

References: None.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD AC-6 (1) (2) (5) (9) (10)	HIGH AC-6 (1) (2) (3) (5) (9) (10)
----	------------------	-------------------------------	------------------------------------

**SYSTEM ADMINISTRATION, NETWORKING, AND SECURITY (SANS)
CONSIDERATION FOR LEAST PRIVILEGE:**

There are many negative factors that affect our cyber lives: massive data loss, intellectual property theft, credit card breaches, and identity theft just to name a few. Cyber defense is rapidly evolving to address the plethora of challenges we face. Defenders have access to a wide array of resources to combat those wishing to do harm. Ranging from the collection of vast amounts of intelligence data to security standards to training and certifications, security practitioners are well armed.

But can information overload actually worsen the problem? Organizations must decide, hopefully based on risk analysis, how to wade through all available resources and select those best suited to their own operating environment. The threats continue to evolve, the attackers become smarter, and user access more mobile. The cloud beckons and can provide reduced cost and infrastructure at a price of less control and accountability for vital information.

The SANS Institute publishes the “20 Critical Security Controls for Effective Cyber Defense”. This list of controls is the combined result of work by an international community to create, adopt, and support the controls. The components of the community provide insight, tools, information, and solutions into threats and adversaries. This list includes the control titled “Controlled Use of Administrative Privileges”. SANS describes this control as: *The process and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.*

Critical Security Control (CSC) 12: Controlled Use of Administrative Privileges

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

ID #	Description	Category
CSC 12--1	Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.	Quick win (<i>One of the “First Five”</i>)
CSC 12--2	Use automated tools to inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive.	Quick win
CSC 12--3	Configure all administrative passwords to be complex and contain letters, numbers, and special characters intermixed, and with no dictionary words present in the password. Pass phrases containing multiple dictionary words, along with special characters, are acceptable if they are of a reasonable length.	Quick win

CSC 12--4	Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration---level accounts.	<i>Quick win</i>
CSC 12--5	Ensure that all service accounts have long and difficult-- to-- guess passwords that are changed on a periodic basis, as is done for traditional user and administrative passwords.	<i>Quick win</i>
CSC 12--6	Passwords should be hashed or encrypted in storage. Passwords that are hashed should be salted and follow guidance provided in NIST SP 800-- 132 or similar guidance. Files containing these encrypted or hashed passwords required for systems to authenticate users should be readable only with super--user privileges.	<i>Quick win</i>
CSC 12--7	Utilize access control lists to ensure that administrative accounts are used only for system administration activities, and not for reading e--mail, composing documents, or surfing the Internet. Web browsers and e--mail clients especially must be configured to never run as administrator.	<i>Quick win</i>
CSC 12--8	Through policy and user awareness, require that administrators establish unique, different passwords for their administrative and non--administrative accounts. Each person requiring administrative access should be given his/her own separate account. Users should only use the Windows "administrator" or UNIX "root" accounts in emergency situations. Domain administration accounts should be used when required for system administration instead of local administrative accounts.	<i>Quick win</i>
CSC 12--9	Configure operating systems so that passwords cannot be re-- used within a timeframe of six months.	<i>Quick win</i>
CSC 12--10	Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators' group, or when a new local administrator account is added on a system.	<i>Visibility/ Attribution</i>
CSC 12--11	Configure systems to issue a log entry and alert when unsuccessful login to an administrative account is attempted.	<i>Visibility/ Attribution</i>

CSC 12--12	Use multifactor authentication for all administrative access, including domain administrative access. Multi-- factor authentication can include a variety of techniques, to include the use of smart cards with certificates, One Time Password (OTP) tokens, and biometrics.	<i>Configuration/ Hygiene</i>
CSC 12--13 (NEW)	When using certificates to enable multi-- factor certificate-- based authentication, ensure that the private keys are protected using strong passwords or are stored in trusted, secure hardware tokens.	<i>Configuration/ Hygiene</i>
CSC 12--14	Block access to a machine (either remotely or locally) for administrator--level accounts. Instead, administrators should be required to access a system using a fully logged and non-- administrative account. Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems. Users would use their own administrative accounts and enter a password each time that is different than their user account.	<i>Configuration/ Hygiene</i>

Quick win: Implementation provides significant risk reduction without major financial, procedural, architectural, or technical changes to an environment, or that provide substantial and immediate risk reduction against very common attacks that most security-aware organizations prioritize these key controls.

Visibility / attribution: Measures to improve the process, architecture, and technical capabilities of organizations to monitor their networks and computer systems to detect attack attempts, locate points of entry, identify already-compromised machines, interrupt infiltrated attackers' activities, and gain information about the sources of an attack.

Configuration / hygiene: reduce the number and magnitude of security vulnerabilities and improve the operations of networked computer systems, with a focus on protecting against poor security practices by system administrators and end-users that could give an attacker an advantage.

SEPARATION OF DUTIES:

Separation of duties is another security control related to least privilege. Many of the same challenges faced by least privilege apply to this concept as well. Agency size and resources play a major in the implementation of separation of duties. As the name implies, some key functions should be separated between different individuals. The goal of this concept is to provide protection

against a single individual's ability to circumvent system security controls to gain unauthorized access or perform unauthorized actions without colluding with other individuals.

Simply put separation of duties entails distributing certain critical mission oriented functions or system administrative support functions amongst different individuals or roles. It also includes delineating information system support duties such as auditing, configuration control, or network security between different individuals.

As with least privilege, an agency's ability to implement separation of duties is typically based on financial and personnel resources. While a very large agency may have ready availability to those resources to ensure critical functions are spread across multiple individuals, a small agency probably does not have that luxury.

THREATS:

What effect can an individual with carte blanc access to all critical functions of a system have? Consider a single individual with the ability to install nefarious applications on a system (e.g. a keylogger). If this same individual also has the ability to edit any audit logs that would have recorded the actions of installing the software, those entries could be deleted and any evidence of the installation eliminated.

Perhaps a disgruntled system administrator wants to open a port on a firewall to allow a remote backdoor connection into the information system in order to siphon off criminal justice information. Because the perpetrator has access to the firewall and all logs, the port can be opened and the logs tampered with to eliminate records of the action.

As mentioned previously, the two concepts of least privilege and separation of duties are related. Additional threats are presented when a system administrator using a single account with unlimited elevated privileges across the information system uses that account to check email. In a successful phishing attack that compromises this account, the attacker now has unrestricted unauthorized access to all system resources and the ability to hide their tracks.

MITIGATION:

The primary method to avoid these situations is to configure system privileges and duties such that a single person is unable to effect questionable change to the system and then are able to erase any evidence of the change.

Technical configurations are most secure and sound enforceable policies compliment the technical solutions. When an information system does not support separating duties, strong policies help mitigate risk.

NIST CONSIDERATIONS FOR SEPARATION OF DUTIES:

NIST Special Publication 800-53 specifies the guidance for separation of duties in the control catalog under the Access Control (AC) family and specifically as AC-5. While the NIST requirements are not enforceable under the CJIS Security Policy, they were the genesis of the Policy and do provide a sound security baseline that can be leveraged by the criminal and noncriminal justice community. AC-5 is a relatively small control with no enhancements but it is significant in protecting the integrity of an information system.

AC-5 Separation of Duties

Control: The organization:

- a. Separates [*Assignment: organization-defined duties of individuals*];
- b. Documents separation of duties of individuals; and
- c. Defines information system access authorizations to support separation of duties.

Supplemental Guidance: Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions. Related controls: AC-3, AC-6, PE-3, PE-4, PS-2.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD AC-5	HIGH AC-5
----	------------------	----------	-----------

G.6 Encryption

Encryption

Purpose:

This paper was created to provide assistance and guidance on encryption types, methods, and to provide general best practices in the implementation of encryption.

Attribution:

- FIPS 140 – 2, Security Requirements for Cryptographic Modules (May 2001)
- FIPS 197, Advanced Encryption Standard (Nov 2001)
- NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices
- CNSSP-15, National Information Assurance Policy on the Use of Public Standards for Secure Sharing of Information among Security Systems
- CJIS Security Policy

Definitions and Terms:

Encryption – A form of cryptology that applies a cryptographic operation to provide confidentiality of (sensitive) information.

Decryption – The inverse cryptographic operation used to convert encrypted information back into a plaintext (readable) format.

Asymmetric Encryption – A type of encryption that uses key pairs for encryption. One key is used to encrypt a message and another key to decrypt the message. Asymmetric encryption is also commonly known as public key encryption.

Symmetric Encryption – A type of encryption where the same key is used to encrypt and decrypt a message. Symmetric encryption is also known as secret key encryption.

Hybrid encryption – A type of encryption where both asymmetric encryption and symmetric encryption keys are used creating what is referred to as cipher suites. In a hybrid solution the asymmetric encryption keys are used for client/server certificate exchange to provide session integrity while the symmetric encryption keys are used for bulk data encryption to provide data confidentiality.

Authorized User/Personnel - An individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI.

Summary :

CJIS Security Policy encryption requirements are intended to provide protection of the sensitive data that is criminal justice information (CJI). The primary goal of encrypting CJI is to prevent unauthorized access to this sensitive data. Encryption is a great tool that can be applied to accomplish this protection and ensure compliance with the vast majority of the CJI requirements. CJIS Security Policy Section 5.10.1.2 details when encryption is required and provides information on the exceptions to the encryption requirement.

Achieving CJIS Security Policy Compliance:

To determine when encryption is required one must first read and understand CJIS Security Policy Section 5.9.1 Physically Secure Location. The reason for this is simple: encryption is not required while within a physically secure location. Conversely, whenever CJI is transmitted or stored (at rest) outside the boundaries of a physically secure location encryption may be required. The exact standards to which the data would be required to meet are detailed along with any exceptions in CJIS Security Policy Section 5.10.1.2.

Additionally, both security awareness training and personnel security requirements can be affected by whether or not CJI is encrypted. Requirements surrounding these Policy areas is determined by answering the following question: Who has unescorted access to unencrypted CJI?

Unless personnel is escorted, security awareness training is required as correlated with the access level needed by personnel as identified in CJIS Security Policy Section 5.2. Similarly, fingerprint-based background checks as detailed in CJIS Security Policy Section 5.12 may be required on individuals to permit unescorted access to CJI.

The intent of all these requirements is to limit access to CJI to only authorized personnel. CJIS Security Policy Appendix A: Terms and Definitions defines authorized user/personnel as an individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI.

What is Encryption?

Encryption is the process of encoding messages or information in such a manner that only people with the knowledge or means to decrypt the message can do so. But how does this work?

In an encryption process, legible data, referred to as plaintext, is encrypted by applying a cipher (otherwise known as an encryption algorithm or crypto key) to the data. The data then becomes encrypted and is now referred to as ciphertext. The ciphertext is essentially unreadable until decrypted. The decryption process requires the process of applying the same algorithm (crypto key) to encrypt the data in an inverse manner to convert the data back into plaintext.

Encryption is important because it allows you to securely protect data that you don't want anyone else to have access to. Encryption has been used throughout history to send “secrets” securely by some form of obfuscation to a recipient. Businesses and enterprises use encryption to protect corporate secrets and sensitive employee data, such as payroll information and personally identifiable information (PII). Governments secure classified information with encryption. Additionally, individuals may use encryption to protect personal information, such as credit card data, banking information, and passwords to guard against things like identity theft.

It should be known that encryption may not always prevent the interception of data. If the stolen data is encrypted, though, it would be extremely difficult for any of the data to be decrypted without having the decryption key. While it may be possible to decrypt the message without possessing the key, it does require large computational resources, great skill, and lots of time to accomplish such a task. Exercising encryption along with key management policies is one of the best security practices that can be put into place with regard to sensitive data security and protection.

Types of Encryption:

Symmetric Encryption

Symmetric encryption is also commonly known as secret key encryption. Symmetric encryption is a form of cryptography utilizing a singular encryption key to guise an electronic message. Its data conversion uses a mathematical algorithm along with a secret key, which results in the inability to make sense out of a message. Symmetric encryption is a two-way algorithm because the mathematical algorithm is reversed when decrypting the message along with using the same secret key.

Symmetric encryption is most often used for data protection whether at rest or in transit, especially in bulk, due to the ease and speed with which the encryption can be implemented. The most common examples of symmetric algorithms are: AES and Triple-DES (3DES or TDEA).

How it works:

To encrypt and send a message to Jane, John does the following:

1. Generates a new symmetric key
2. Encrypts the message using this new symmetric key
3. Sends the message to Jane
4. Sends the encrypted symmetric key to Jane - out of band

To decrypt this ciphertext, Jane does the following:

1. Receives the encrypted message
2. Receives the symmetric key
3. Uses the symmetric key to decrypt the message

Asymmetric Encryption

Asymmetric encryption is also commonly known as public-key encryption. Asymmetric cryptography is cryptography in which a pair of keys, a public key and a private key, are used to encrypt and decrypt a message so that it arrives securely. Initially, a network user receives a public and private key pair from a certificate authority. Any other user who wants to send an encrypted message can get the intended recipient's public key from a public directory. They use this key to encrypt the message, and they send it to the recipient. When the recipient gets the message, they decrypt it with their private key, which no one else should have access to.

Creating Key Pairs:

Asymmetric encryption requires the use of algorithms of great computational complexity to create the key pairs. This is accomplished by using a large, random number that an algorithm is applied to which generates a pair of keys for use as asymmetric key algorithms (as shown in Figure 1 below).

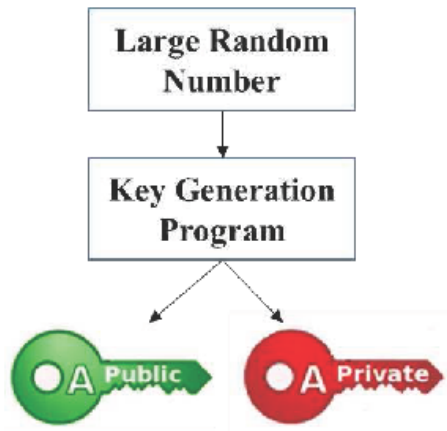


Figure 1 – Asymmetric key pair generation

Asymmetric encryption is most often used to encrypt a single message before transmission. The most common examples of asymmetric algorithms are: RSA and DSA.

How it works:

To encrypt and send a message to Jane, John does the following:

1. Obtains Jane's public key
2. Encrypts the message using Jane's public key
3. Sends the message to Jane

To decrypt this ciphertext, Jane does the following:

1. Receives the encrypted message
2. Uses her private key to decrypt the message

Advantages of Using Symmetric Encryption for Data Protection

Asymmetric encryption requires the use of algorithms with great computational complexity to create the key pairs, and therefore is not practical for large amounts of data. It is typically used for only for short messages. Also, asymmetric encryption must use a comparatively stronger key than symmetric key encryption to achieve the same level of protection as one key (public) will be published in the public directory for all to see.

Symmetric encryption is based on large, but simple algorithms which require less computation. Therefore, is much faster to create and use keys. This allows the same key to be used to encrypt and decrypt the message. So, data can be encrypted in real time. The (shared) key is sent to the recipient out of band so that it can be used to decrypt the data.

For the reasons stated above, symmetric key encryption is the preferred choice by both industry and government alike to encrypt large amounts of data (bulk encryption) simply due to the ease and real time encryption capabilities as detailed above. Additionally, a new key can be generated for every session, message transaction, etc., as desired. This means a sender won't have to use one key (public) to encrypt a message and have the recipient use another key (private) to decrypt the message.

Hybrid Encryption

Hybrid encryption solution exist where both asymmetric encryption and symmetric encryption keys are used to create what is referred to as cipher suites. In a hybrid solution the asymmetric encryption keys are used for client/server certificate exchange to provide session integrity while the symmetric encryption keys are used for bulk data encryption to provide data confidentiality.

Hybrid solutions are most often used by Internet browsers to protect data in transit. The most common examples of hybrid encryption are: TLS/SSL, PGP, IPSEC, and S/MIME.

How it works:

To encrypt a message to Jane in a hybrid cryptosystem, John does the following:

1. Obtains Jane's public key
2. Generates a new symmetric key
3. Encrypts the message using this new symmetric key
4. Encrypts the symmetric key using Jane's public key
5. Sends the message to Jane

To decrypt this hybrid cipher text, Jane does the following:

1. Receives the encrypted message
2. Receives the encrypted symmetric key
3. Uses her private key to decrypt the symmetric key
4. Uses the symmetric key to decrypt the message

Explaining Cipher Suites:

A cipher suite is a set of cryptographic algorithms used for the following:

- Protect information required to create shared keys (key exchange)
- Encrypt messages exchanged between clients and servers (bulk encryption)
- Generate message hashes and signatures to ensure the integrity of a message (message authentication)

Examples of Transport Layer Security (TLS) 1.2 Cipher Suites:

- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

A cipher suite specifies one algorithm for each of the above tasks. For example, the TLS_RSA_WITH_AES_128_SHA256 cipher suite is used for TLS. The suite uses the RSA asymmetric algorithm for key exchange, AES with a 128-bit key for bulk data encryption, and SHA256 for message authentication.

Symmetric and Asymmetric Key Strength Comparison:

<u>Symmetric</u>		<u>Asymmetric</u>		
<u>Bits of security</u>	<u>Symmetric key algorithms</u>	<u>Finite-Field Cryptography (FFC)</u> <u>(e.g., DSA, D-H)</u> <u>Bits of security</u>	<u>Integer-Factorization Cryptography (IFC)</u> <u>(e.g., RSA)</u> <u>Bits of security</u>	<u>Elliptic-Curve Cryptography (ECC)</u> <u>(e.g., ECDSA)</u> <u>Bits of security</u>
<u>80</u>	<u>2TDEA18</u>	<u>Public key = 1024</u> <u>Private key = 160</u>	<u>Key size = 1024</u>	<u>Key size = 160-223</u>
<u>112</u>	<u>3TDEA</u>	<u>Public key = 2048</u> <u>Private key = 224</u>	<u>Key size = 2048</u>	<u>Key size = 224-255</u>
<u>128</u>	<u>AES-128</u>	<u>Public Key = 3072</u> <u>Private key = 256</u>	<u>Key size = 3072</u>	<u>Key size = 256-383</u>
<u>192</u>	<u>AES-192</u>	<u>Public key = 7680</u> <u>Private key = 384</u>	<u>Key size = 7680</u>	<u>Key size = 384-511</u>
<u>256</u>	<u>AES-256</u>	<u>Public key = 15360</u> <u>Private key = 512</u>	<u>Key size = 15360</u>	<u>Key size = 512+</u>

Figure 2 - Symmetric and asymmetric key strength comparison

As you can see in the chart provided above, the equivalent key strengths between symmetric and asymmetric key strengths do not necessarily correlate. There is a reason for this. As stated previously, asymmetric algorithms must use a comparatively stronger key than symmetric key encryption to achieve the same strength. The simplest explanation for this is because one of the keys is published to the public directory and can constantly be attacked by anyone with access to the directory. Therefore, the public key must be made of such strength that it can resist getting compromised while made public.

Federal Information Processing Standard (FIPS) 140-2 Explained

Origin of FIPS 140-2

On July 17, 1995, the National Institute of Standards and Technology (NIST) established the Cryptographic Module Validation Program (CMVP) to validate cryptographic modules to Federal Information Processing Standards (FIPS) Security Requirements for Cryptographic Modules, and other FIPS cryptography based standards. The CMVP is a joint effort between NIST and the Communications Security Establishment Canada (CSEC). FIPS 140-2, Security Requirements for Cryptographic Modules, was released on May 25, 2001 to supersede the original FIPS 140-1. Modules validated as conforming to FIPS 140-1 and FIPS 140-2 are accepted by the Federal Agencies of both countries for the protection of sensitive information.

What is FIPS 140-2?

Federal Information Processing Standard (FIPS) is a standard developed and recommended (often mandated) for use in federal-government-operated IT systems by the following two government bodies:

- The National Institute of Standards and Technology (NIST) in the United States
- The Communications Security Establishment (CSE) in Canada

FIPS 140-2 specifies the security requirements a cryptographic module must meet when utilized within a security system protecting sensitive information within information systems (computer and telecommunication systems). FIPS 140-2 specifies which encryption algorithms can be used and how encryption keys are to be generated and managed.

How does a product get certified?

Vendors of cryptographic modules can have their products tested by independent, accredited Cryptographic and Security Testing (CST) laboratories. The CST laboratories use the Derived Test

Requirements (DTR), Implementation Guidance (IG) and applicable CMVP programmatic guidance to test cryptographic modules against the applicable standards in a variety of implementations. The result of these tests are reported to NIST's Computer Security Division (CSD) and CSEC who jointly serve as the Validation Authorities for the program. These results are then reviewed and certificates would be issued if the results are determined to be acceptable.

What is the difference between being FIPS 140-2 compliant and being FIPS 140-2 certified?

It is common theme to discover a product is "FIPS compliant." What does this mean, though? The difference between compliance and certification is not subtle. Certification requires a vast testing, verification, and validation process be performed by a CST laboratory as described in the previous section. Compliance is merely a claim stating the implementation of an encryption solution is done in accordance with the security policy related to the FIPS certification. Any claim of compliance would need to be validated and the corresponding certificate number would have to be known.

NIST has addressed related claims as shown below in their Frequently Asked Questions for the Cryptographic Module Validation Program:

A vendor makes the following claims of conformance to FIPS 140-2. Are they acceptable?

- The module has been designed for compliance to FIPS 140-2. <NO>
- Module has been pre-validated and is on the CMVP pre-validation list. <NO>
- The module will be submitted for testing. <NO>
- The module has been independently reviewed and tested to comply with FIPS 140-2. <NO>
- The module meets all the requirements of FIPS 140-2. <NO>
- The module implements FIPS Approved algorithms; including having algorithm certificates. <NO>
- The module follows the guidelines detailed in FIPS 140-2. <NO>
- The module has been validated and has received Certificate #XXXXX. <YES>

A cryptographic module does not meet the requirements or conform to the FIPS 140-2 standard unless a reference can be made to the validation certificate number. The module used must also be the same version/part number as annotated on the validation certificate. Any other claims are not relevant.

To read more FAQs from NIST on FIPS certification, use the following NIST website link:
<http://csrc.nist.gov/groups/STM/cmvp/documents/CMVPFAQ.pdf>

Where can I learn more about FIPS 140-2?

For more information about the FIPS 140-2 standard, go to the following NIST website:
<http://csrc.nist.gov/cryptval/140-2.htm>

General Recommendations:

Encryption key management control is of paramount importance! Agencies should develop policies and procedures define and monitor the administrative tasks involved with protection, storage, organization, access controls and the lifecycle management of encryption keys. After all, encryption keys should not be accessible by just anyone. An encryption key management control process should ensure only authorized users have access to encryption keys. Key management is a best security practice and helps to ensure the confidentiality and integrity of CJI data and enforces key access control.

The CJIS Security Policy is a “living” document under constant review and receiving regular updates through the Advisory Policy Board (APB) process. Agencies need to always keep up to date on the latest requirements. These requirements can be found in CJIS Security Policy Section 5.10.1.2. Please contact the CJIS ISO Program anytime to address any questions or concerns about CJIS Security Policy requirements, the current APB status of CJIS Security Policy requirements, or if seeking general information or guidance.

G.7 Incident Response

Incident Response

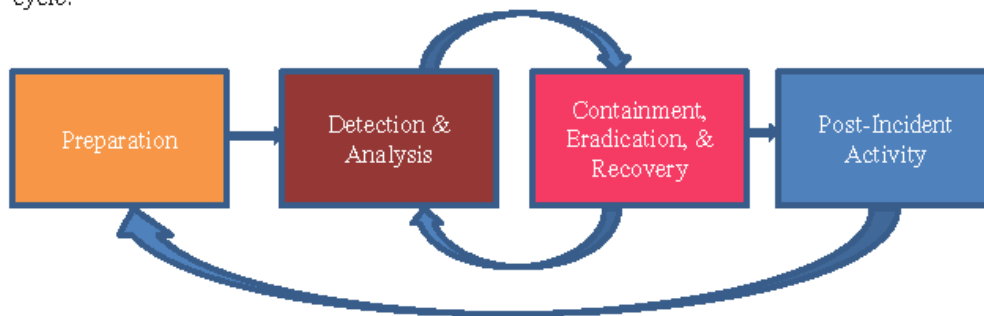
Introduction

Information technology (IT) security incident response is an important and critical component of information technology programs. Performing incident response effectively can be a complex undertaking – for that reason, establishing a successful incident response capability requires planning and resources. Everyone in an organization must be aware of IT security risks, threats, and actions to take in situations where an actual IT security incident has occurred. Even the best-secured and controlled environments can experience these security risks, threats, events, and incidents. This document provides guidelines for appropriate response to IT security incidents, and are independent of specific hardware platforms, operating systems, protocols, or applications.

The following example incidents are used to highlight appropriate actions during each phase:

- Malicious code execution
- Ransomware execution
- Denial of service attack
- Social Engineering
- Phishing

NIST Special Publication 800-61 rev. 2 outlines the “Incident Response Life Cycle” as a collection of phases – distinct sets of activities that will assist in the handling of a computer security incident, from start to finish. The following diagram explains the process flow of the incident response life cycle:



Preparation

The initial phase of the incident response life cycle, “Preparation”, involves establishing and training an incident response team, and acquiring the necessary tools and resources. A computer security incident may not have happened at this phase, but it is important to utilize all available knowledge and security measures to obtain the best posture for responding to potential future incidents. One of the most important preparation steps involves the collection, storage, and accessibility of event data and telemetry from hardware and software resources such as firewall logs, application logs, operating system logs, and other valuable sources of situational data, as well as the output of products that perform analysis on such data. Preventive measures to mitigate or eliminate future incidents are deployed during this phase, using industry best practices, data obtained from research and intelligence sources, and lessons learned from past incidents.

It is also imperative to prepare a list of contact information or notification methodologies to employ when an incident occurs, as well as notification and communication strategies within the team, with stakeholders, and with upper management and potentially other criminal justice and non-criminal justice agencies. This will help ensure that when incidents arise, the proper personnel and organizations are notified and kept informed of the circumstances regarding the incident.

Using the example incident categories outlined earlier, some overview into appropriate actions and activities for the Preparation phase can be given:

Malicious code execution

Preparation for incidents involving malicious code execution should initially involve user awareness of sources of malicious code. There are many potential sources of malicious code, such as web pages, emails, and removable media. The utilization and deployment of effective antivirus software, integrity-monitoring software, and intrusion detection and prevention software are effective measures to take to prepare for incidents involving malicious code execution.

Ransomware execution

Preparation phase activities for incidents involving ransomware execution are much the same as activities for malicious code execution, as ransomware is a specialized form of malware that encrypts potentially important or critical files, with the intention of coercing a victim to pay for a decryption key. Implementing a robust offline backup solution for these types of files is an important preparative action to take regarding the execution of ransomware. This will ensure that when ransomware attacks do happen, the mission impact is as minimal as possible and very little or no data is lost.

Denial of service attack

Denial of service attacks are given attention in the preparation phase. Defensive responses to denial of service attacks typically involve the use of a combination of attack detection and traffic classification and response tools, aiming to block traffic identified as abusive denial of service activity. Deploying solutions such as IDS/IPS devices and software, network hardware with rate-limiting capabilities (routers, switches, and firewalls), and upstream filtering devices at the system perimeter can mitigate for denial of service attacks.

Social Engineering

Preparation for social engineering attacks starts with user awareness training. Understanding and identifying attempts to obtain information in an unauthorized manner is crucial to thwarting these types of scenarios. Social engineering is the art of manipulating people to obtain information they may not be authorized to handle. Training and routinely testing users on potential social engineering scenarios and tactics, and providing training regarding appropriate responses to requests involving personal or otherwise sensitive information (for example, passwords or criminal justice information), is an effective way to ensure social engineering attacks never traverse past the preparation phase of the incident response life cycle.

Phishing

Like social engineering, preparation for phishing attacks is imperative. Phishing is a social engineering technique attackers employ to deceive users, in a fraudulent attempt to obtain sensitive information, or to gain unauthorized access to systems. Phishing is extremely widespread, and attackers disguising fraudulent scenarios in electronic communication such as email and instant messages are the most common. User awareness of these types of tactics is paramount to prepare for phishing attacks and schemes.

Detection and Analysis

The detection and analysis phase begins when a security incident has occurred. To understand when this phase begins, there must be a capability for an intelligent determination of circumstances constituting a security incident. Specialized knowledge and highly trained personnel are necessary for this step to be effective. Many organizations employ teams of personnel who are specifically trained to handle the intricacies of the incident response life cycle. The determination of a security incident can arise from one or several circumstances simultaneously – for example:

- Trained personnel manually reviewing collected event data for evidence of compromise
- Software applications analyzing events, trends, and patterns of behavior
- The observation of suspicious or anomalous activity on a computer system

The goals of this phase are:

- To detect whether a security incident occurred
- To determine the vector (i.e., method) of attack
- To determine the impact of the incident to the mission, systems, and personnel involved in the incident
- To obtain or create intelligence products regarding attack vectors and methodologies, especially when dealing with malicious code

Prioritization of incidents is also an important decision point in the incident response life cycle, as the circumstances regarding an incident can bring the situation to a critical level. There are three major impacts to consider when addressing priority of incidents:

- Functional Impact: the impact to business functionality
- Information Impact: the impact to confidentiality, integrity, and/or availability of criminal justice information
- Recoverability: the amount of time and resources that must be spent on recovering from an incident

Documentation regarding an incident should be thorough and applicable to the incident. This can be crucial in incidents that may lead to legal prosecution, as well as being invaluable to efficiently document, track, handle, manage, and resolve one or more incidents at the same time.

Using the example incident categories outlined earlier, some overview into appropriate actions and activities for the Detection and Analysis phase are given:

Malicious code execution

Detection of malicious code execution is often a primary job of host-based antivirus software. Having a capable and up-to-date antivirus solution installed on a system can detect known malicious code, as well as detect potentially malicious behaviors. The delivery of malicious code to a system can be detected by network traffic analysis and protection tools and hardware. Additionally, some malicious code may produce network traffic that is indicative of successful execution, exploitation, and/or compromise of a system. Solutions such as intrusion detection/prevention systems, Security Information and Event Management (SIEM) tools, and file integrity monitoring software can provide the necessary level of fidelity to make a determination of malicious code execution.

Knowing if or when a system is infected is not always immediately evident. Security controls may have been bypassed or even disabled by the malicious code. However, systems infected by malicious code or software (i.e. malware) can exhibit several indicators. These indicators include, but are not limited to:

Unexpected pop-up windows

- Slow start up and/or slow performance
- Suspicious hard drive activity including an unexpected lack of storage space
- Missing files
- Crashes and/or error messages
- Unexplained network activity
- Hijacked email

Analysis of malicious code can be performed in several ways. Static analysis of malicious code can be performed to determine the capabilities of the malicious code and generate actionable intelligence. Dynamic analysis of malicious code can be used to observe how the malicious code interacts with the system and what actions it performs and can often more rapidly determine the capabilities of malicious code. Both static and dynamic analysis can be performed manually, as well as in an automated fashion. Trained specialized personnel are crucial to the analysis of malicious code.

Ransomware execution

The detection of ransomware is identical to the detection of malicious code. Ransomware is specialized malicious code that encrypts potentially valuable files, generally with the intent to coerce a victim to pay a ransom for the possibility of the decryption of those files. Host-based antivirus solutions can also detect these threats, and network traffic analysis and protection tools and hardware can be used to prevent the successful execution of ransomware. SIEM tools and file integrity monitoring software can also detect the execution of ransomware.

Analysis of ransomware is identical to the analysis of malicious code, and the same intelligence can be determined in the same fashion as with the analysis of malicious code. The most obvious sign that ransomware has affected a system is the existence of encrypted files, the disappearance of certain types of files, and/or the presence of “ransom notes” on the system, which contain instructions for payment to obtain a decryption key, which may or may not be legitimate.

Denial of service attack

Denial of service (DoS) attacks are often detected at the perimeter of an organization but can also be detected within the organization as well. Often, from a user’s perspective, the signs of a DoS attack appear to be network performance or administrative maintenance related issues such as slow or broken network connections or down websites. Additionally, an administrator may notice ping time outs, event logs overflowing or alerts from network monitoring systems as issues that may identify a DoS attack. Intrusion detection and prevention software and platforms can detect denial of service attacks, as well as some network monitoring hardware and appliances, such as web application filters, routers,

firewalls, and switches. Devices targeted by denial of service attacks can also detect the attacks in some instances, if they have the capabilities to determine explicit attack activity versus normal network traffic.

Analysis of denial of service attacks include the determination of the source traffic, the protocols used to generate the traffic, the service(s) targeted by the attack, and the potential impacts of the attack. Network monitoring devices can often provide these types of data, with the exception of potential impacts of denial of service attacks on systems.

Social Engineering

Detection of social engineering attacks is primarily based on the situational awareness of the individual targeted by social engineering. Given that social engineering is a broad topic that can involve the manipulation and exploitation of people in control of an information system, user awareness of social engineering attempts is crucial. If the target has security awareness training in detecting attempts to gain information or access in an unapproved manner, social engineering is easier to detect.

Analysis of social engineering attacks will generally rely on the recollection abilities of or documentation taken by the targets of the attack. Social engineering may not occur on an information system and may be completely carried out in-person. If the target can recollect or produce documentation regarding the social engineering attempt, the motivation and desired access can potentially be determined. For successful social engineering attempts, recollection and documentation of the attempt is crucial to determining the level of unauthorized access that was obtained.

Phishing

Detection of phishing attacks generally will first occur at an organization's email point of presence. Some organizations still run their own email servers, and many have migrated to cloud solutions. Having an on-premise email server or server farm or cluster will require additional functionality to detect phishing attempts. For example, the header content of the email will need to be read, as well as the content inside the body of the email, to check for potentially malicious content and potentially falsified data that may indicate a phishing email. Many cloud email providers have built this capability into their email solutions, but it is still possible for users to receive phishing emails, as attacker tactics and capabilities evolve daily. The most effective detection of phishing comes from heightened situational awareness of potential attacks. Validating the source of the email can uncover potential phishing attempts.

Analysis of phishing attacks involves examination of email headers, as well as contents of the body of the email. The body of the email may contain malicious content, attachments, or links to suspicious or malicious content. Manual or automated analysis activities can be

performed on the email content. Analysis of these elements should be performed by trained specialized personnel to generate intelligence and aid with the determination of indicators of compromise.

Containment, Eradication, and Recovery

Containment activities for computer security incidents involve decision-making and the application of strategies to help control attacks and damage, cease attack activities, or reduce the impact or damage caused by the incident. Often, this requires intelligence gathered by the detection and analysis phases of the incident – for example, identification of affected hosts, identification of attacking hosts or attackers, identification of malware and its capabilities, and identification and monitoring of attacker communication channels can be invaluable to the implementation of containment activities. In most cases, it is important to introduce containment solutions all at once, as attackers may escalate their attack activity if deployment of the strategy is delayed.

Eradication efforts for a computer security incident involve removal of latent threats from systems (such as malware on the system and user accounts that may have been created), identifying and mitigating potential vulnerabilities or misconfigurations that may have been exploited, and identification of other hosts that may have been affected within the organization.

Recovery efforts for incidents involve restoration of affected systems to normal operation. This may include actions like restoring systems from backups, rebuilding systems from an agency-approved baseline, replacing compromised files with clean versions, installing patches, changing passwords, and increasing network perimeter and host-based security.

Compromised hosts are often attacked during these phases, as attackers try to regain their foothold on compromised systems or systems on the same network or others in the logical vicinity.

Malicious code execution

Containment activities for malicious code execution involve the logical or physical isolation of the host from the attacker's control and from any mission services or systems that would be impacted by the compromised host. This may include putting the host in a restricted VLAN, using firewalls to block traffic, disconnecting it from the network completely, shutting it down, or disabling functionality. Exercise caution as malicious code may have capabilities to take further actions on a host in case communications with a command and control server are severed. It is important to understand the capabilities of the malicious code before taking containment actions.

Eradication activities include the removal of malicious code from the system. This may be as simple as removing files, configuration rules, accounts, and other persistent items that the malicious code utilizes to function and maintain a presence on the system. This phase

also involves the discovery and removal of indicators of compromise on other systems, if applicable. It is imperative to remediate vulnerabilities that may have been exploited during eradication as well.

Recovery from malicious code execution generally is similar across many environments. Rebuilding the system from a clean baseline or restoring files from backup are typical activities that help restore the functionality of the system to continue the mission. Changing system passwords, installing patches, implementing tighter network access control, and ensuring appropriate levels of logging fidelity of the information system are integral parts of the recovery process.

Ransomware execution

Containment for ransomware execution should be as swift and immediate as possible, as ransomware can execute and spread to accessible media at a rapid pace. Considering files are being encrypted or have already been encrypted, immediate action should be taken to logically or physically isolate the system by disconnecting network connectivity. It is up to the system owner whether to take the risk in powering off the system, as valuable forensic artifacts may be destroyed in the process, but it will halt the execution of the ransomware and protect potentially valuable files. Please note that containment of active ransomware execution is one of the only circumstances where measures such as immediate shutdown are recommended.

Eradication of ransomware does not need to occur in most circumstances, as the entire goal of ransomware is to encrypt files and leave “recovery” instructions to extort victims. The vast majority of ransomware will delete itself once encryption of files is complete, but it is possible that some ransomware is persistent and can remain on the system. If this is the case, analysis should be performed on the ransomware to determine its capabilities, and eradication activities will proceed in an identical fashion to malicious code execution eradication activities.

Recovery from ransomware execution involves restoring encrypted files from backup and may involve the rebuilding of an entire system depending on the extent of the encryption from the ransomware. If a robust offline backup solution for hosts is not present or not utilized on a regular basis, the loss of potentially valuable data may be incredibly costly in several areas to repair, to include man-hours, revenue, and business products, data, and intelligence.

Denial of service attack

Containment of denial of service attacks involve the modification of access control where the attack is occurring. For example, if a web or application server is experiencing a denial of service attack, the system itself, as well as network monitoring devices, should be

examined to determine the source of the attack traffic. Once the source of the traffic is identified, modifications to access controls or rate-limiting features such as firewall access controls lists (ACLs) and web application filters can be employed to block the traffic. Care must be taken to determine if the observed traffic is actually intentional malicious denial of service traffic, versus heavy legitimate network traffic. Implementing access control mechanisms or rate-limiting features may negatively affect the mission of the system. It is also important to note that manual containment in this fashion may not be entirely effective, as attackers can circumvent the ACL by changing the attacking IP address, protocol, or other attribute of the connection.

Eradication is not necessarily applicable in denial of service scenarios, unless a vulnerability or misconfiguration is being exploited to cause the denial of service condition. If this is the case, take steps to remediate the vulnerability or misconfiguration.

Recovery actions depend on the available resources of the information system. For example, on-premise load balancers can be used to distribute the traffic, whether legitimate or malicious, to other less-burdened systems. Many cloud providers and content delivery networks also have denial of service mitigation capabilities. It may also be prudent to increase the resources (memory, processing capacity) of internet-facing systems so that they can handle larger amounts of traffic simultaneously.

Social Engineering

Containment regarding social engineering attacks is dependent upon the information or access that was provided to the attacker. For example, if an attacker gained access to an account on a system following a social engineering attempt, the account should be administratively disabled and all sources of event data regarding that account should be immediately collected. If sensitive data was divulged to the attacker, the impact of the exposure of that data should be examined and mitigating activity should be initiated to determine or reduce the damage of the spread of the information.

Eradication regarding social engineering attacks also depends on the information or access provided to the attacker. Removing or limiting the provided access is a pertinent eradication action. If the information provided is a credential to a system, disable and remove the credential from the system. Eradication may also involve the physical detainment or removal of personnel from a site.

Recovery actions for social engineering attacks are dependent on the information or access provided to the attacker. Additionally, security awareness training is an appropriate recovery action to ensure staff understands the threats of social engineering.

Phishing

Containment of phishing activity is tied very closely to the identification and analysis of the phishing activity. Understanding the tactics of the phishing attacker is paramount to deploying containment activities. Activities include, but are not limited to, administratively blocking sender email addresses and IPs, blocking potential malicious content in email via a web proxy, communicating with potential recipients, and implementation of email content or hyperlink blacklisting if possible. Phishing attacks can also include attempts to have users execute malicious code on systems, where containment activities regarding malicious code will be applicable.

Eradication of phishing attacks include the administrative removal of the emails from email systems, as well as eradication actions for malicious code if applicable.

Recovery from phishing attacks can include:

- Implementation and enforcement of the Domain Keys Identified Mail (DKIM) email authentication method, which can mitigate the possibility that attackers can send spoofed email
- Implementation and enforcement of Sender Policy Framework (SPF) to control and stop sender forgeries
- Implementation and enforcement of Domain-based Message Authentication, Reporting, and Conformance (DMARC), which enables message senders to indicate that their messages are protected with SPF and/or DKIM

Additionally, if malicious code is present in the phishing attack, recovery actions regarding malicious code may be applicable.

Post-Incident Activity

Post-incident activities occur after the detection, analysis, containment, eradication, and recovery from a computer security incident. Arguably one of the most important phases of incident response, post-incident activities involve the reflection, compilation, and analysis of the activities that occurred leading to the security incident, and the actions taken by those involved in the security incident, including the incident response team. Some of the important items to consider:

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?

- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar actions in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Smaller incidents, and those that are similar to others that have been well documented, do not necessarily need much focus in this phase of incident response. Larger and less-understood security incidents should be the focus of a comprehensive post-mortem evaluation that outlines many of the items listed above and should include personnel that can have a direct impact on or are directly affected or responsible for the involved systems.

Post-incident activities such as these also help to serve as training opportunities for all parties involved in the incident, from victims, to system administration personnel, to incident responders.

Malicious code execution

Post-incident activities for malicious code execution generally will follow similar patterns. A timeline of activity should have been prepared using digital forensic data collected during the detection and analysis phases of the incident. This timeline should include all affected systems and times of all activities and actions taken during the incident. Steps that victims and system administrators may have taken during the course of the incident, as well as in close proximity to the time range of the incident, are valuable items to document and discuss. Any deviation from organizational policy should be noted and taken as training items or assigned consequences in accordance with organizational policies. It may also be pertinent to ensure that appropriate information and intelligence sharing was performed during and after the incident occurred. Corrective actions that may have prevented the execution of malicious code, such as antivirus solutions, restrictions on where executables can run, tightened permissions, and script blockers for browsers, should be considered as a mitigation for the risks posed by malicious code threats. Web proxy blocks from information discovered during analysis can be utilized to ensure that malicious hosts are not contacted.

Ransomware execution

Post-incident activities for ransomware execution include all the activities involved with malicious code execution, with the addition of ensuring the functionality of a robust offline backup solution. An offline backup solution ensures that backup data is kept inaccessible to ransomware threats and is available if ransomware is successfully executed. A functional and frequent (such as daily incremental and weekly full) backup process helps ensure that business continuity is maintained in the event of issues and incidents.

Denial of service attack

Denial of service post-incident activities should include a timeline of traffic activities, as well as organizational responses to the attack traffic as well as the timeline of any business impacts and the damage associated with the impacts. Any attack precursors should be investigated and noted, and intelligence implemented to notify personnel and potentially take action as soon as attack traffic is observed. Impacts on affected systems should be noted, and a consensus should be reached on whether the systems should be upgraded or supplemented with load-balancing capabilities.

Social Engineering

Post-incident activities for social engineering incidents should include a timeline that includes all applicable activities, such as points of contact, narratives from the parties involved, CCTV footage (if applicable), system and network log files, and physical access control logging data. If unauthorized access was obtained, the impact of the access should be assessed and mitigating factors should be identified for inclusion to reduce the risk of future incidents (such as multifactor authentication, physical locks, greater CCTV coverage, improved physical access control, etc.). Security awareness training should be imperative if policy was breached, and information or access was given to unauthorized parties.

Phishing

Phishing post-incident activities should also include a timeline of actions taken since the phishing email was received, to include descriptions of the type of phishing campaign observed (malicious code, financial exploitation, credential harvesting, etc.), malicious attachments contained (if any), malicious or suspicious links in the body of emails, as well as narratives from recipients of the email and any potential victims, either self-reported or discovered through email, network, or host-based monitoring. If malicious code was included in the campaign, typical post-incident activities involving malicious code should be considered as well. Training opportunities can often arise from phishing attacks, whether successful or not, that can be valuable in giving employees better situational awareness regarding phishing.

The CJIS Security Policy requires each agency with access to CJIS to establish operational incident handling procedures (i.e. a local policy). Gleaning from the requirements in Section 5.3 Incident Response, the local policy may include the following elements:

- Overall incident handling procedures. This section describes and identifies the processes used locally how the agency successfully prepares for, manages, and recovers from an incident. It includes sections on:
 - Preparation
 - Detection and Analysis
 - Containment

- Recovery
 - User response activities
- How the agency performs incident reporting. This section describes the process of notifying internal and external partners when an incident has occurred and how the incident is documented. It includes sections on:
 - Internal and external points of contact
 - Required tracking and reporting documents
 - Escalation procedures
- Incident management procedures. This section describes the agency's approach to a consistent and repeatable approach to managing incidents. It includes sections on:
 - Roles and responsibilities
 - Incident-related information collection
 - Updating policies with lessons learned
 - Collection of evidence
 - Incident response training
 - Document and artifact retention

G.8 Secure Coding

Secure Coding

This appendix documents a source of information on best practices and standards for secure coding. With the increased use of software products and the rapid pace of modern software development, it is essential to discover and resolve insecure software risks. The mitigations and guidelines to reduce these common risks can be found in secure coding best practices.

Understanding how software applications work can be a daunting thing; however, it could be key to know if data security is in jeopardy. Awareness of secure coding practices allows an agency to review potential vendors and their products prior to purchase and implementation. It also empowers the agency with the knowledge of the questions to ask a vendor of how the software was developed and whether the vendor uses secure coding practices or standards.

Additionally, the information in this appendix can provide a path forward for agencies with the internal capability to produce “in-house” software applications. By implementing security during the code writing process, security is “baked in” and there is more trust the software will aid in protecting the information it processes.

Open Web Application Security Project (OWASP) Foundation

The OWASP Foundation is a not-for-profit charitable organization focused on improving the security of software. OWASP operates as a community of like-minded professionals to provide unbiased and practical information about application security (AppSec) through software tools and documentation. These materials are available under a free and open software license, which can be located at the link below.

https://www.owasp.org/index.php/Main_Page

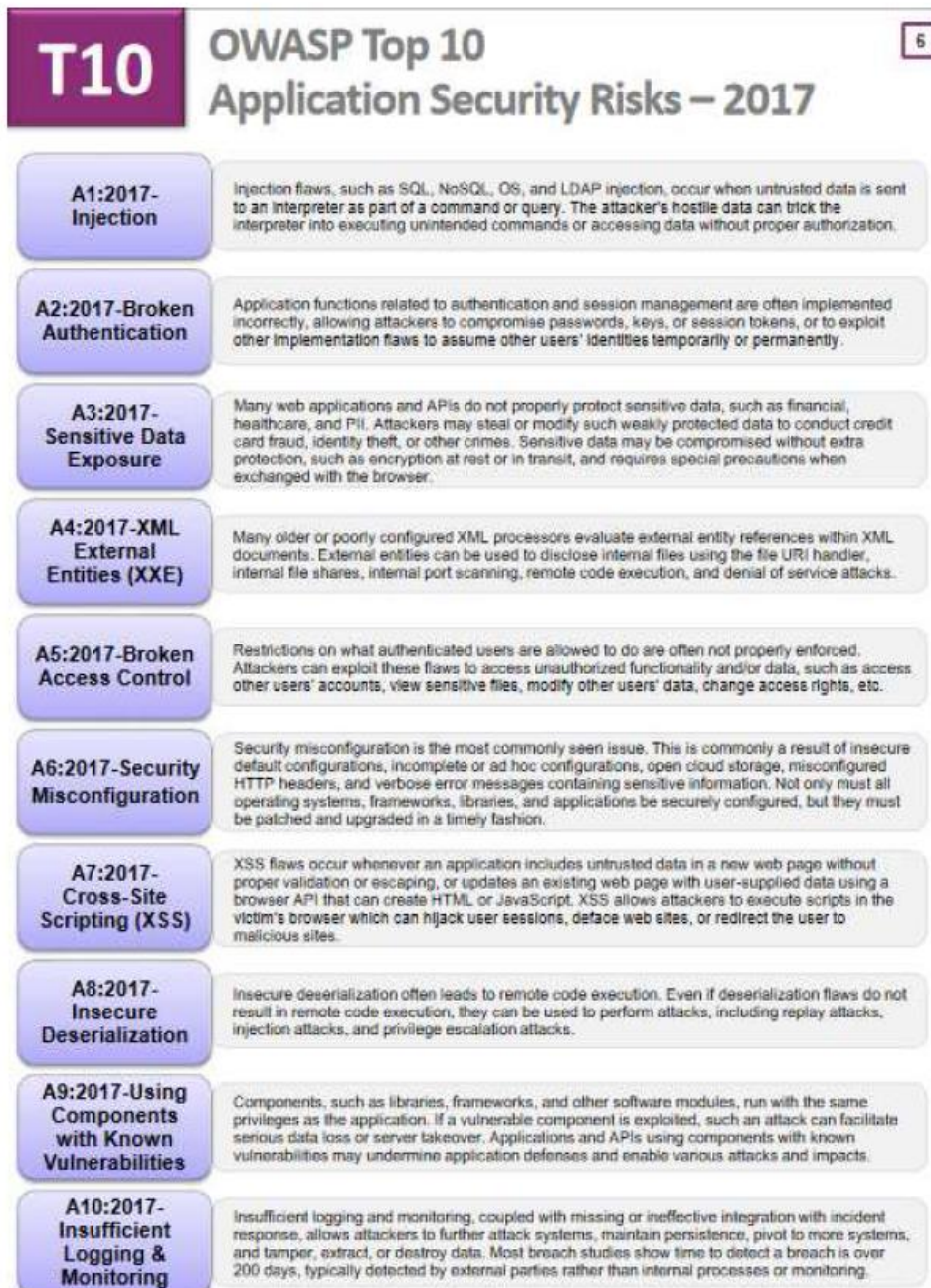
Software is becoming increasingly complex and connected, and the difficulty of achieving application security increases exponentially. The rapid pace of modern software development processes makes the most common risks essential to discover and resolve quickly and accurately.

The OWASP Foundation publishes the Top 10 Application Security Risks, which focus on the most serious web application security risks. The OWASP Top 10 is based primarily on 40 plus data submissions from firms that specialize in application security and an industry survey that was completed by over 500 individuals. This data spans vulnerabilities gathered from hundreds of organizations and over 100,000 real world applications and application program interfaces (API). The Top 10 items are selected and prioritized according to this data, in combination with consensus estimates of exploitability, detectability, and impact.

A primary aim of the OWASP Top 10 is to educate developers, designers, architects, managers, and organizations about the consequences of the most common and most important web application security weaknesses. The Top 10 provides basic techniques to protect against these high risks problem areas, and provides guidance on a path forward.

The OWASP Top 10 focuses on identifying the most serious web application security risks for a broad array of organizations. For each of these risks, generic information about likelihood and technical impact using the following simple ratings scheme, which is based on the OWASP Risk Rating Methodology.

Figure G.8-A



Each organization is unique, and so are the threat actors for that organization, their goals, and the impact of any breach. It is critical to understand the risk to your organization based on applicable threat agents and business impacts.

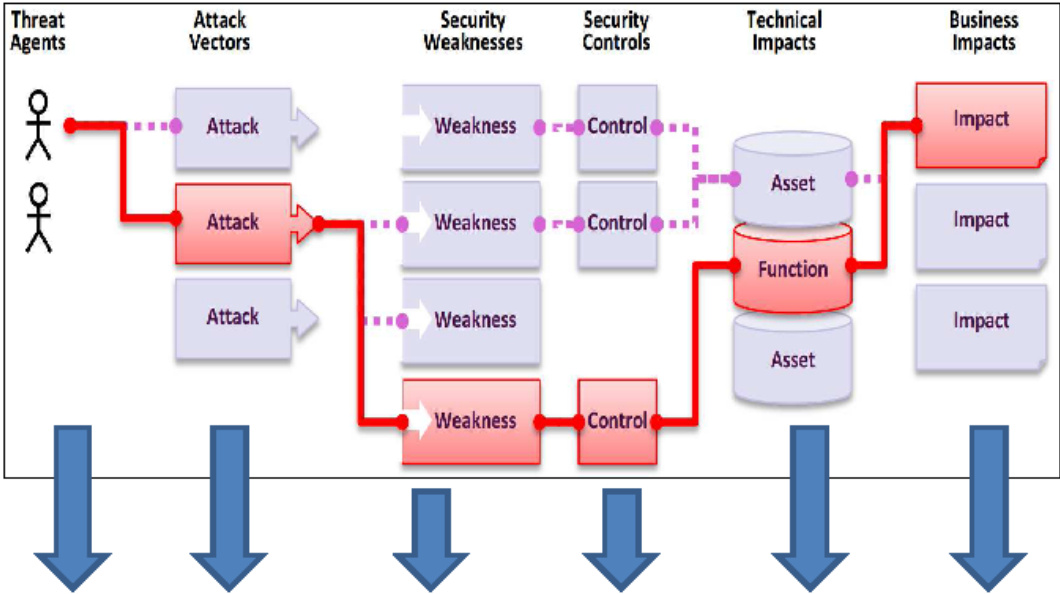
Application Security Risks

The figures immediately below illustrate the path of a sample threat beginning with the threat agent and ending with the target or affected business resource. Various paths are available but the agent would normally select the path of least resistance which would be the most vulnerable and with the fewest number of effective security controls.

The sample risk matrix can be used to assign in the various aspects of potential vulnerability. Each column corresponds to a phase in the attack process. In the matrix, a lower value represents less risk and is more desirable.

Concerning secure coding practices, when security is built-in during code development, vulnerabilities can be identified and controls included reducing the overall risk to information processed by the code.

Figure G.8-B Sample Threat Path







Threat Agents	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impacts	Business Impacts
App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	SEVERE: 3	App / Business Specific
	AVERAGE: 2	COMMON: 2	AVERAGE: 2	MODERATE: 2	
	DIFFICULT: 1	UNCOMMON: 1	DIFFICULT: 1	MINOR: 1	

Figure G.8-C General Risk Matrix

To understand these risks for a particular application or organization, you must consider your own specific threat agents and business impacts. Even severe software weaknesses may not present a serious risk if there are no threat agents in a position to perform the necessary attack or the business impact is negligible for the assets involved. The following table presents a summary of the 2017 Top 10 Application Security Risks, and the risk factors that have been assigned to each risk.

Figure G.8-D. Top 10 Risk Factor Summary

RISK	 Threat Agents	 Attack Vectors	 Security Weakness			 Impacts	Score
	Exploitability	Prevalence	Detectability	Technical	Business		
A1:2017- Injection	App Specific	EASY: 3	COMMON: 2	EASY: 3	SEVERE: 3	App Specific	8.0
A2:2017- Authentication	App Specific	EASY: 3	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	7.0
A3:2017 Sens. Data Exposure	App Specific	AVERAGE: 2	WIDESPREAD: 3	AVERAGE: 2	SEVERE: 3	App Specific	7.0
A4:2017-XML External Entities (XXE)	App Specific	AVERAGE: 2	COMMON: 2	EASY: 3	SEVERE: 3	App Specific	7.0
A5:2017-Broken Access Control	App Specific	AVERAGE: 2	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	6.0
A6:2017-Security Misconfiguration	App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	MODERATE: 2	App Specific	6.0
A7:2017 Cross Site Scripting (XSS)	App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	MODERATE: 2	App Specific	6.0
A8:2017-Insecure Deserialization	App Specific	DIFFICULT: 1	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	5.0
A9:2017-Vulnerable Components	App Specific	AVERAGE: 2	WIDESPREAD: 3	AVERAGE: 2	MODERATE: 2	App Specific	4.7
A10:2017-Insufficient Logging&Monitoring	App Specific	AVERAGE: 2	WIDESPREAD: 3	DIFFICULT: 1	MODERATE: 2	App Specific	4.0

Whether you are new to web application security or already very familiar with these risks, the task of producing a secure web application or fixing an existing one can be difficult. If you have to manage a large application portfolio, this task can be daunting.

To help organizations, developers, testers and managers reduce their application security risks in a cost-effective manner; OWASP has produced numerous free and open resources that you can use to address application security in your organization. The following are some of the many resources OWASP has produced to help organizations produce secure web applications and APIs.

Get Started:

- Document all applications and associated data assets.
- Larger organizations should consider implementing a Configuration Management Database (CMDB).
- Establish an application security program to conduct analysis to define key improvement areas and an execution plan.

Risk Based Portfolio Approach:

- Identify the protection needs of your application portfolio from a business perspective.
- Establish a common risk-rating model with a consistent set of likelihood and impact factors reflective of your organization's tolerance for risk.
- Measure and prioritize all applications and APIs and add results to CMDB.

Enable with a Strong Foundation:

- Establish a set of policies and standards that provide an application security baseline for all development teams to adhere too.
- Define a common set of reusable security controls that complement these policies and standards and provide design and development guidance on their use.

Integrate Security into Existing Processes:

- Define and integrate secure implementation and verification activities into existing development and operational processes.
 - Activities include threat modeling, secure design and design review, secure coding and code review, penetration testing, and remediation.

Application Security Requirements - to produce a secure web application, you must define what secure means for that application.

- [Application Security Verification Standard \(ASVS\):](https://www.owasp.org/index.php/ASVS)
<https://www.owasp.org/index.php/ASVS>
- [OWASP Secure Software Contract Annex:](https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex)
https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex

Application Security Architecture - retrofitting security into your applications and APIs, it is far more cost effective to design the security in from the start.

- OWASP Prevention Cheat Sheets:

https://www.owasp.org/index.php/OWASP_Cheat_Sheet_Series

Standard Security Controls - building strong and usable security controls is difficult. Using a set of standard security controls radically simplifies the development of secure applications and APIs.

- OWASP Proactive Controls:
https://www.owasp.org/index.php/OWASP_Proactive_Controls

Secure Development Lifecycle - to improve the process your organization follows when building applications and APIs, organizations formulate and implement a strategy for software security that is tailored to the specific risks facing their organization.

- OWASP Software Assurance Maturity Model (SAMM):
https://www.owasp.org/index.php/OWASP_SAMM_Project
- OWASP Application Security Guide for CISOs:
https://www.owasp.org/index.php/Application_Security_Guide_For_CISOs

Application Security Education – hands-on learning about vulnerabilities to help educate developers on web application security.

- OWASP Education Project:
https://www.owasp.org/index.php/Category:OWASP_Education_Project
- OWASP WebGoat:
<https://www.owasp.org/index.php/WebGoat>
- OWASP Broken Web Application Project:
https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project

Understand the Threat Model – be sure to understand the priorities when it comes to threat model.

- OWASP Testing Guide:
https://www.owasp.org/index.php/OWASP_Testing_Project
- Application Security Verification Standard (ASVS):
<https://www.owasp.org/index.php/ASVS>

Testing Strategies – choose the simplest, fastest, most accurate technique to verify each requirement.

- OWASP Security Knowledge Framework:
https://www.owasp.org/index.php/OWASP_Security_Knowledge_Framework

- [Application Security Verification Standard \(ASVS\):
https://www.owasp.org/index.php/ASVS](https://www.owasp.org/index.php/ASVS)

APPENDIX H SECURITY ADDENDUM

The following pages contain the legal authority, purpose, and genesis of the Criminal Justice Information Services Security Addendum (H2-H4); the Security Addendum itself (H5-H6); and the Security Addendum Certification page (H7).

**FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM**

**Legal Authority for and Purpose and Genesis of the
Security Addendum**

Traditionally, law enforcement and other criminal justice agencies have been responsible for the confidentiality of their information. Accordingly, until mid-1999, the Code of Federal Regulations Title 28, Part 20, subpart C, and the National Crime Information Center (NCIC) policy paper approved December 6, 1982, required that the management and exchange of criminal justice information be performed by a criminal justice agency or, in certain circumstances, by a noncriminal justice agency under the management control of a criminal justice agency.

In light of the increasing desire of governmental agencies to contract with private entities to perform administration of criminal justice functions, the FBI sought and obtained approval from the United States Department of Justice (DOJ) to permit such privatization of traditional law enforcement functions under certain controlled circumstances. In the Federal Register of May 10, 1999, the FBI published a Notice of Proposed Rulemaking, announcing as follows:

1. Access to CHRI [Criminal History Record Information] and Related Information, Subject to Appropriate Controls, by a Private Contractor Pursuant to a Specific Agreement with an Authorized Governmental Agency To Perform an Administration of Criminal Justice Function (Privatization). Section 534 of title 28 of the United States Code authorizes the Attorney General to exchange identification, criminal identification, crime, and other records for the official use of authorized officials of the federal government, the states, cities, and penal and other institutions. This statute also provides, however, that such exchanges are subject to cancellation if dissemination is made outside the receiving departments or related agencies. Agencies authorized access to CHRI traditionally have been hesitant to disclose that information, even in furtherance of authorized criminal justice functions, to anyone other than actual agency employees lest such disclosure be viewed as unauthorized. In recent years, however, governmental agencies seeking greater efficiency and economy have become increasingly interested in obtaining support services for the administration of criminal justice from the private sector. With the concurrence of the FBI's Criminal Justice Information Services (CJIS) Advisory Policy Board, the DOJ has concluded that disclosures to private persons and entities providing support services for criminal justice agencies may, when subject to appropriate controls, properly be viewed as permissible disclosures for purposes of compliance with 28 U.S.C. 534.

We are therefore proposing to revise 28 CFR 20.33(a)(7) to provide express authority for such arrangements. The proposed authority is similar to the authority that already exists in 28 CFR 20.21(b)(3) for state and local CHRI systems. Provision of CHRI under this authority would only be permitted pursuant to a specific agreement with an authorized governmental agency for the purpose of providing services for the administration of criminal justice. The agreement would be required to incorporate a security addendum approved by the Director of the FBI (acting for the Attorney General). The security

addendum would specifically authorize access to CHRI, limit the use of the information to the specific purposes for which it is being provided, ensure the security and confidentiality of the information consistent with applicable laws and regulations, provide for sanctions, and contain such other provisions as the Director of the FBI (acting for the Attorney General) may require. The security addendum, buttressed by ongoing audit programs of both the FBI and the sponsoring governmental agency, will provide an appropriate balance between the benefits of privatization, protection of individual privacy interests, and preservation of the security of the FBI's CHRI systems.

The FBI will develop a security addendum to be made available to interested governmental agencies. We anticipate that the security addendum will include physical and personnel security constraints historically required by NCIC security practices and other programmatic requirements, together with personal integrity and electronic security provisions comparable to those in NCIC User Agreements between the FBI and criminal justice agencies, and in existing Management Control Agreements between criminal justice agencies and noncriminal justice governmental entities. The security addendum will make clear that access to CHRI will be limited to those officers and employees of the private contractor or its subcontractor who require the information to properly perform services for the sponsoring governmental agency, and that the service provider may not access, modify, use, or disseminate such information for inconsistent or unauthorized purposes.

Consistent with such intent, Title 28 of the Code of Federal Regulations (C.F.R.) was amended to read:

§ 20.33 Dissemination of criminal history record information.

- a) Criminal history record information contained in the Interstate Identification Index (III) System and the Fingerprint Identification Records System (FIRS) may be made available:
 - 1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies.
 - 2) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies; and
 - 3) To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain such other provisions as the Attorney General may require. The power

and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

This Security Addendum, appended to and incorporated by reference in a government-private sector contract entered into for such purpose, is intended to insure that the benefits of privatization are not attained with any accompanying degradation in the security of the national system of criminal records accessed by the contracting private party. This Security Addendum addresses both concerns for personal integrity and electronic security which have been addressed in previously executed user agreements and management control agreements.

A government agency may privatize functions traditionally performed by criminal justice agencies (or noncriminal justice agencies acting under a management control agreement), subject to the terms of this Security Addendum. If privatized, access by a private contractor's personnel to NCIC data and other CJIS information is restricted to only that necessary to perform the privatized tasks consistent with the government agency's function and the focus of the contract. If privatized the contractor may not access, modify, use or disseminate such data in any manner not expressly authorized by the government agency in consultation with the FBI.

**FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM**

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

- a. Investigate or decline to investigate any report of unauthorized use;
- b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer

Criminal Justice Information Services Division, FBI

1000 Custer Hollow Road

Clarksburg, West Virginia 26306

**FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM**

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

Printed Name/Signature of Contractor Employee

Date

Printed Name/Signature of Contractor Representative

Date

Organization and Title of Contractor Representative

APPENDIX I REFERENCES

- White House Memo entitled "Designation and Sharing of Controlled Unclassified Information (CUI)", May 9, 2008
- [CJIS RA] *CJIS Security Policy Risk Assessment Report*; August 2008; For Official Use Only; Prepared by: Noblis; Prepared for: U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, 1000 Custer Hollow Road, Clarksburg, WV 26306
- [CNSS Instruction No. 4009] *National Information Assurance (IA) Glossary*; Committee on National Security Systems (CNSS) Instruction No. 4009; 26 April 2010
- [FBI SA 8/2006] *Federal Bureau of Investigation, Criminal Justice Information Services, Security Addendum*; 8/2006; Assistant Director, Criminal Justice Information Services, FBI, 1000 Custer Hollow Road, Clarksburg, West Virginia 26306
- [FISMA] *Federal Information Security Management Act of 2002*; House of Representatives Bill 2458, Title III–Information Security
- [FIPS 199] *Standards for Security Categorization of Federal Information and Information Systems*; Federal Information Processing Standards Publication, FIPS PUB 199; February 2004
- [FIPS 200] *Minimum Security Requirements for Federal Information and Information Systems*; Federal Information Processing Standards Publication, FIPS PUB 200; March 2006
- [FIPS 201] *Personal Identity Verification for Federal Employees and Contractors*; Federal Information Processing Standards Publication, FIPS PUB 201-1
- [NIST SP 800–14] *Generally Accepted Principles and Practices for Securing Information Technology Systems*; NIST Special Publication 800–14
- [NIST SP 800–25] *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*; NIST Special Publication 800–25
- [NIST SP 800–30] *Risk Management Guide for Information Technology Systems*; NIST Special Publication 800–36
- [NIST SP 800–32] *Introduction to Public Key Technology and the Federal PKI Infrastructure*; NIST Special Publication 800–32
- [NIST SP 800–34] *Contingency Planning Guide for Information Technology Systems*; NIST Special Publication 800–34
- [NIST SP 800–35] *Guide to Information Technology Security Services*; NIST Special Publication 800–35
- [NIST SP 800–36] *Guide to Selecting Information Technology Security Products*; NIST Special Publication 800–36
- [NIST SP 800–39] *Managing Risk from Information Systems, An Organizational Perspective*; NIST Special Publication 800–39
- [NIST SP 800–40] *Procedures for Handling Security Patches*; NIST Special Publication 800–40

- [NIST SP 800-44] *Guidelines on Securing Public Web Servers*; NIST Special Publication 800-44
- [NIST SP 800-45] *Guidelines on Electronic Mail Security*; NIST Special Publication 800-45, Version 2
- [NIST SP 800-46] *Security for Telecommuting and Broadband Communications*; NIST Special Publication 800-46
- [NIST SP 800-48] *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*; NIST Special Publication 800-48
- [NIST SP 800-52] *Guidelines on the Selection and Use of Transport Layer Security*; NIST Special Publication 800-52
- [NIST SP 800-53] *Recommended Security Controls for Federal Information Systems*; NIST Special Publication 800-53, Revision 2
- [NIST SP 800-53A] *Guide for Assessing the Security Controls in Federal Information Systems, Building Effective Security Assessment Plans*; NIST Special Publication 800-53A
- [NIST SP 800-58] *Security Considerations for Voice over IP Systems*; NIST Special Publication 800-58
- [NIST SP 800-60] *Guide for Mapping Types of Information and Information Systems to Security Categories*; NIST Special Publication 800-60, Revision 1, DRAFT
- [NIST SP 800-63-1] *Electronic Authentication Guideline*; NIST Special Publication 800-63-1; DRAFT
- [NIST SP 800-64] NIST Special Publication 800-64
- [NIST SP 800-66] *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA)*; NIST Special Publication 800-66
- [NIST SP 800-68] *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*; NIST Special Publication 800-68
- [NIST SP 800-70] *Security Configuration Checklists Program for IT Products*; NIST Special Publication 800-70
- [NIST SP 800-72] *Guidelines on PDA Forensics*; NIST Special Publication 800-72
- [NIST SP 800-73] *Integrated Circuit Card for Personal Identification Verification*; NIST Special Publication 800-73; Revision 1
- [NIST SP 800-76] *Biometric Data Specification for Personal Identity Verification*; NIST Special Publication 800-76
- [NIST SP 800-77] *Guide to IPSec VPNs*; NIST Special Publication 800-77
- [NIST SP 800-78] *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*; NIST Special Publication 800-78
- [NIST SP 800-81] *Secure Domain Name System (DNS) Deployment Guide*; NIST Special Publication 800-81
- [NIST SP 800-84] *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*; NIST Special Publication 800-84

- [NIST SP 800-86] *Guide to Integrating Forensic Techniques into Incident Response*; NIST Special Publication 800-86
- [NIST SP 800-87] *Codes for the Identification of Federal and Federally Assisted Agencies*; NIST Special Publication 800-87
- [NIST SP 800-96] *PIV Card / Reader Interoperability Guidelines*; NIST Special Publication 800-96
- [NIST SP 800-97] *Guide to IEEE 802.11i: Robust Security Networks*; NIST Special Publication 800-97
- [NIST SP 800-121] *Guide to Bluetooth Security*; NIST Special Publication 800-121
- [NIST SP 800-124] *Guidelines on Cell Phone and PDA Security*; NIST Special Publication 800-124
- [NIST SP 800-125] *Guide to Security for Full Virtualization Technologies*; NIST Special Publication 800-125
- [NIST SP 800-144] *Guidelines on Security and Privacy in Public Cloud Computing*; NIST Special Publication 800-144
- [NIST SP 800-145] *The NIST Definition of Cloud Computing*; NIST Special Publication 800-145
- [NIST SP 800-146] *Cloud Computing Synopsis and Recommendations*; NIST Special Publication 800-146
- [OMB A-130] *Management of Federal Information Resources*; Circular No. A-130; Revised; February 8, 1996
- [OMB M-04-04] *E-Authentication Guidance for Federal Agencies*; OMB Memo 04-04; December 16, 2003
- [OMB M-06-15] *Safeguarding Personally Identifiable Information*; OMB Memo 06-15; May 22, 2006
- [OMB M-06-16] *Protection of Sensitive Agency Information*; OMB Memo 06-16; June 23, 2006
- [OMB M-06-19] *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*; OMB Memo 06-19; July 12, 2006
- [OMB M-07-16] *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*; OMB Memo 07-16; May 22, 2007
- [Surviving Security] *Surviving Security: How to Integrate People, Process, and Technology*; Second Edition; 2004
- [USC Title 5, Section 552] *Public information; agency rules, opinions, orders, records, and proceedings*; United States Code, Title 5 - Government Agency and Employees, Part I - The Agencies Generally, Chapter 5 - Administrative Procedure, Subchapter II - Administrative Procedure, Section 552. Public information; agency rules, opinions, orders, records, and proceedings

[USC Title 44, Section 3506] *Federal Information Policy*; 01/02/2006; United States Code,
Title 44 - Public Printing and Documents; Chapter 35 - Coordination of
Federal Information Policy; Subchapter I - Federal Information Policy, Section
3506

APPENDIX J NONCRIMINAL JUSTICE AGENCY SUPPLEMENTAL GUIDANCE

This appendix is not intended to be used in lieu of the CJIS Security Policy (CSP) but rather should be used as supplemental guidance specifically for those Noncriminal Justice Agencies (NCJA) with access to Criminal Justice Information (CJI) as authorized by legislative enactment or federal executive order to request civil fingerprint-based background checks for licensing, employment, or other noncriminal justice purposes, via their State Identification Bureau (SIB) and/or Channeling agency. Examples of the target audience for the Appendix J supplemental guidance include school boards, banks, medical boards, gaming commissions, alcohol and tobacco control boards, social services agencies, pharmacy boards, etc.

The CSP is the minimum standard policy used by both criminal and noncriminal justice agencies requiring access to CJI maintained by the FBI CJIS Division. The essential premise of the CSP is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CSP provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

For those NCJAs new to the CSP and Advisory Policy Board (APB) auditing process (all NCJAs will be periodically audited by the CJIS Systems Agency (CSA)/SIB and may be included in a sampling of triennial audits conducted by the FBI) it is strongly recommended that each system processing CJI should be individually reviewed to determine which CSP requirements may apply. In the interim however this supplemental guidance provides a minimum starting point that every NCJA processing CJI can immediately put into place. Once the broader array of security controls are gleaned for a specific system, agencies can then leverage the (already implemented) controls described in this appendix as a launching pad towards full policy compliance.

The following information is organized to provide the section and section title within the CSP, along with a brief summary and background on the guidance itself. For the specific “shall” statement please go to the referenced section within the main body of the CSP.

General CJI Guidance

The following information provides NCJAs guidance to maintain security compliance when setting up any system capable of sending and/or receiving CJI:

a. **3.2.9 – Local Agency Security Officer (LASO)**

It is the responsibility of the CJIS Systems Officer (CSO) to ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO) per CSP Section 3.2.2(2e).

The LASO serves as the primary point of contact (POC) between the local NCJA and their respective CSA CSO or Information Security Officer (ISO) who interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to information security, disseminates information security alerts and other material to their constituents, maintains information security documentation (including system configuration data), assists with Information Security audits of hardware and

procedures, and keeps the CSA (i.e., CSO or ISO) informed as to any information security needs and problems.

b. 5.1.1.6 – Agency User Agreements

When an NCJA (private or public) is permitted to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions as authorized pursuant to federal law or state statute approved by the U.S. Attorney General, the information received from the background check, such as criminal history record information (CHRI) or personally identifiable information (PII), must be protected as CJI. In order to receive access to CJI the NCJA must enter into a signed written agreement, i.e., an agency user agreement, with the appropriate signatory authority of the CSA, SIB, or authorized agency providing the CJI access. An example of a NCJA (private) is a local bank. An example of a NCJA (public) is a county school board.

Note 1: The CSA, SIB, or authorized agency providing the CJI access term should be part of the agency user agreement.

Note 2: Any NCJA that directly accesses FBI CJIS must allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system.

c. 5.1.3 – Secondary Dissemination

Secondary dissemination is the promulgation of CJI from a releasing agency to an authorized recipient agency that has not been previously identified in a formal information exchange agreement.

If CHRI is released to another authorized agency, that is not part of the releasing agency's primary information exchange agreement(s), the releasing agency must log such dissemination.

d. 5.2.1.1 – All Personnel (Security Awareness Training)

Basic security awareness training is required for all personnel who have access to CJI within six months of initial assignment, and biennially thereafter. CSP Section 5.2.1.1 describes the topics that must be addressed within baseline security awareness training for all authorized personnel with access to CJI.

Note: The CSO/SIB may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.

e. 5.3 – Incident Response

CSP Section 5.3 assists agencies with response and reporting procedures for accidental and malicious computer and network attacks. The requirements within Section 5.3 will help NCJAs with:

- (i) Establishing an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and,
- (ii) Tracking, documenting, and reporting incidents to appropriate agency officials and/or authorities.

CSP Section 5.3.1 describes the requirements for reporting security events and describes the responsibilities of the FBI CJIS Division and the CSA ISO.

CSP Section 5.3.2 describes the requirements for managing security incidents, to include: incident handling and the collection of evidence.

CSP Section 5.3.3 describes the requirement for an agency to ensure general incident response roles responsibilities are included as part of required security awareness training.

CSP Section 5.3.4 describes the requirement for an agency to track and document information system security incidents on an ongoing basis.

Note 1: CSA ISOs serve as the POC on security-related issues for their respective agencies and must ensure LASOs institute the CSA incident response reporting procedures at the local level. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.

Note 2: CSP Appendix F contains a sample incident notification letter for use when communicating the details of an incident to the FBI CJIS ISO.

f. 5.4 – Auditing and Accountability

CSP Section 5.4 assists agencies in assessing the inventory of components that compose their information systems to determine which security controls are applicable to the various components and implement required audit and accountability controls.

CSP Section 5.4.1 describes the required parameters for agencies to generate audit records and content for defined events and periodically review and update the list of agency-defined auditable events.

CSP Section 5.4.2 describes the requirement for agencies to provide alerts to appropriate agency officials in the event of an audit processing failure, such as software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

CSP Section 5.4.3 describes the requirements for audit review/analysis frequency and to designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions.

CSP Section 5.4.4 describes the requirement to establish information system time stamp parameters for use in audit record generation.

CSP Section 5.4.5 describes the requirement to protect audit information and audit tools from modification, deletion and unauthorized access.

CSP Section 5.4.6 describes the requirement for an agency to retain audit records for at least one (1) year.

Note: The agency will continue to retain audit records for longer than one (1) year until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes - for example, retention and availability of audit records relative

to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.

CSP Section 5.4.7 describes the requirements for logging National Crime Information Center (NCIC) and Interstate Identification Index (III) transactions. A log must be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log will clearly identify both the operator and the authorized receiving agency. III logs must also clearly identify the requester and the secondary recipient. The identification on the log will take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one (1) year retention period.

g. 5.8 – Media Protection

CJIS Security Policy Section 5.8 assists agencies to document and implement media protection policy and procedures required to ensure that access to electronic and physical media in all forms is restricted to authorized individuals for securely handling, transporting and storing media.

“Electronic media” is electronic storage media, such as memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card. “Physical media” refers to CJI in physical form, e.g. printed documents, printed imagery, etc.

CSP Section 5.8.1 describes the requirement for agencies to securely store electronic and physical media within physically secure locations or controlled areas and restrict access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data must be encrypted per CSP Section 5.10.1.2.

CSP Section 5.8.2 describes the requirements for agencies to protect and control both electronic and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel. The agency is responsible for implementing controls to protect electronic media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in CSP Section 5.10.1.2, is the optimal control; however, if encryption of the data isn’t possible then each agency must institute other controls to ensure the security of the data.

CSP Section 5.8.3 describes the requirements for agencies to maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies must sanitize (electronically overwrite the data at least three times) or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. This sanitization or destruction needs to be witnessed or carried out only by authorized personnel. Inoperable electronic media must be destroyed (cut up, shredded, etc.).

CSP Section 5.8.4 describes the requirements for physical media to be securely disposed of when no longer required, using established formal procedures. Physical media must be destroyed by shredding or incineration. This disposal or destruction needs to be witnessed or carried out only by authorized personnel.

h. 5.9 Physical Protection

CSP Section 5.9 explains the physical protection policy and procedures that are required to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

CSP Section 5.9.1 details the requirements for establishing a Physically Secure Location - a facility, a criminal justice conveyance, an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. Sections 5.9.1.1 – 5.9.1.8 describe the physical control requirements that must be implemented in order to establish a physically secure location.

CSP Section 5.9.2 details the requirements for establishing a Controlled Area. The controlled area is an area, a room, or a storage container established for the purpose of day-to-day CJI access, storage, or processing in the event an agency is unable to meet all of the controls required for establishing a physically secure location. Access to the controlled area needs to be restricted to only authorized personnel whenever CJI is processed. The CJI material needs to be locked away when unattended to prevent unauthorized and unintentional access. Additionally, the encryption standards of CSP Section 5.10.1.2 apply to the electronic storage (i.e. data “at rest”) of CJI.

i. 5.11 – Formal Audits

CSP Section 5.11 explains the formal audit process to help agencies understand the audit procedures.

CSP Section 5.11.1 details the requirements for compliance and security audits by the FBI CJIS Division. The FBI CJIS Division is authorized to conduct audits, once every three (3) years as a minimum, to assess agency compliance with applicable statutes, regulations and policies.

The CJIS Audit Unit (CAU) will conduct triennial audits of each CSA in order to verify compliance with applicable statutes, regulations and policies. This audit includes a sample of Criminal Justice Agency (CJA) and NCJAs, in coordination with the SIB.

Note 1: Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies.

Note 2: The FBI CJIS Division has the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

CSP Section 5.11.2 describes the requirements for the CSA to triennially audit all CJAs and NCJAs with direct access to the state system, establish a process to periodically audit all NCJAs with access to CJI, establish the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

CSP Section 5.11.3 describes the requirement that all agencies with access to CJI must permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team, appointed by the APB, will include at least one representative of the CJIS Division. All results of the inquiry and audit will be reported to the APB with appropriate recommendations.

Agencies located within states having passed legislation authorizing or requiring civil fingerprint-based background checks for personnel with access to criminal history record

information for the purposes of licensing or employment need to follow the guidance in Section 5.12 (referenced below).

j. 5.12 – Personnel Security

CSP Section 5.12 provides agencies the security terms and requirements as they apply to all personnel who have unescorted access to unencrypted CJI, including individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

CSP Section 5.12.1 details the minimum screening requirements for all individuals requiring unescorted access to unencrypted CJI.

CSP Section 5.12.2 describes the requirement for an agency to immediately terminate CJI access for an individual upon termination of employment.

CSP Section 5.12.3 describes the requirement for an agency to review CJI access authorizations and initiate appropriate actions (such as closing and establishing accounts and changing system access authorizations) whenever personnel are reassigned or transferred to other positions within the agency.

CSP Section 5.12.4 describes the requirement for an agency to employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

Agencies located within states that have not passed legislation authorizing or requiring civil fingerprint-based background checks are exempted from this requirement until such time as appropriate legislation has been written into law.

The following scenarios are intended to help the reader identify areas within the CSP that NCJAs may often come across. Each scenario should be reviewed for applicability in conjunction with the above General CJI Guidance section. The specific requirements found with the CSP are not shown; however specific sections are referenced along with a requirements summary.

Hard Copy CJI Storage and Accessibility

When an NCJA receives CJI via a paper copy from a CJA and stores the paper within a locked file cabinet, the NCJA should, in addition to the General CJI Guidance, focus on compliance with policy section:

a. 4.2.4 – Storage

When storing CJI, appropriate administrative, technical, and physical safeguards must be implemented to ensure the security and confidentiality of the information.

Electronic CJI Storage and Accessibility – Controlled Area

When an NCJA creates an electronic copy of CJI (e.g. scanning a document or creation of a spreadsheet) and subsequently stores this static CJI on either a local hard drive or shared network drive in a controlled area for indirect access by Authorized Recipients, the NCJA should, in addition to the General CJI Guidance, focus on compliance with policy section:

a. 5.5.2.4 (3) – Access Control – Encryption

CSP Section 5.5.2.4 item 3 – Encryption describes the requirement for utilizing encryption as the primary access control mechanism which is necessary in this situation. Encrypted information can only be read by personnel possessing the

appropriate cryptographic key (e.g., passphrase) to decrypt. Refer to Section 5.10.1.2 for specific encryption requirements.

Electronic CJI Storage and Accessibility – Physically Secure Location

When an NCJA receives or creates an electronic copy of CJI and subsequently stores this CJI within a Records Management System (RMS), located within a physically secure location that may be queried by Authorized Recipients, the NCJA should, in addition to the General CJI Guidance, focus on compliance with policy sections:

a. **5.5 – Access Control**

CSP Section 5.5 describes the requirements and parameters for utilizing access control mechanisms for restricting CJI access (such as the reading, writing, processing and transmission of CJIS information) and the modification of information systems, applications, services and communication configurations allowing access to CJI to only authorized personnel.

b. **5.6 – Identification and Authentication**

CSP Section 5.6 describes the requirements and parameters agencies must implement to validate and authenticate the identity of information system users and processes acting on behalf of users the identities prior to granting access to CJI or agency information systems/services that process CJI.

c. **5.7 – Configuration Management**

CSP Section 5.7 describes the requirements for implementing access restrictions that will only permit authorized and qualified individuals access to information system components for purposes of initiating changes, including upgrades, and modifications.

CSP Section 5.7.1 describes the requirements for implementing the concept of least privilege (5.7.1.1) and for developing and maintaining network diagrams (5.7.1.2) that detail how the RMS is interconnected and protected within the network. See Appendix C for sample network diagrams.

CSP Section 5.7.2 details the requirement for agencies to protect the system documentation from unauthorized access consistent with the provisions described in Section 5.5 Access Control.

d. **5.10 – System and Communications Protection and Information Integrity**

CSP Section 5.10 details the requirements for network infrastructures within physically secure locations through establishment of system and communication boundary and transmission protection safeguards that assist in securing an agency's environment, even when virtualized. In addition, this section describes the requirements for providing the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information for applications, services, and information systems.

Use Case Scenarios

1. **Indirect Access to Criminal Justice Information (CJI) Stored on a Network Server**

A county board of education is converting all employee records, including background check information containing CJI, to an electronic format. The records will be scanned from hard copy to electronic files and placed on network server that has indirect access to CJI and is located in a secure data center within the board of education offices. The data center meets all the requirements to be labeled a physically secure location as defined in Section 5.9.1 of the CSP.

Keeping in mind the scenario as described, an authorized user needs access to an employee's electronic record. This user is not located in the secure data center and will have to use remote access to access the file. The user is therefore required to provide identification and authentication credentials to prove they are an authorized user. To access the record, the user is prompted to enter their unique username and password. Because the record resides on a system with indirect access to CJI (does not allow the user to query a state or national criminal record repository), AA is not required to access the record.

NOTE: If the Authorized User has direct access to CJI (the ability to query a state or national criminal record repository) in the above scenario, AA would be required.

2. Encryption for Data at Rest (Exemption for FIPS 140-2 Certified Encryption)

A county board of education is converting all employee records, including background check information containing CJI, to an electronic format. The records will be scanned from hard copy to electronic files and placed on network server that is not located in a secure data center. Because the data center does not meet the requirements of a physically secure location, as defined in Section 5.9.1 of the CSP, the files, at rest (in storage) on the server, are required to be encrypted.

To prevent unauthorized access, the IT staff has decided to encrypt the entire folder that contains the files. They will use a product that provides an advanced encryption standard (AES) encryption algorithm at 256 bit strength to comply with the CSP and employ a CSP compliant passphrase to lock the folder's encryption. When an authorized user needs to access an employee's record, they access the folder on the server and are prompted to enter the designated passphrase to decrypt (unlock) the folder. The user can then access all files within the folder.

NOTE: Whenever authorized personnel no longer require access to the encrypted folder, the passphrase must be changed to prevent future access by that user.

APPENDIX K CRIMINAL JUSTICE AGENCY SUPPLEMENTAL GUIDANCE

This appendix is not intended to be used in lieu of the CJIS Security Policy (CSP) but rather should be used as supplemental guidance specifically for those Criminal Justice Agencies (CJA) that have historically not been subject to audit under the CJIS Security Policy guidelines. The target audience typically gains access to CJI via fax, hardcopy distribution or voice calls; does not have the capability to query state or national databases for criminal justice information; and may have been assigned an originating agency identifier (ORI) but is dependent on other agencies to run queries on their behalf. This guidance is not intended for criminal justice agencies covered under an active information exchange agreement with another agency for direct or indirect connectivity to the state CJIS Systems Agency (CSA) – in other words those agencies traditionally identified as “terminal agencies”.

The CSP is the minimum standard policy used by both criminal and noncriminal justice agencies requiring access to criminal justice information (CJI) maintained by the FBI CJIS Division. The essential premise of the CSP is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CSP provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

For those CJAs new to the CSP it is strongly recommended that each system processing CJI should be individually reviewed to determine which CSP requirements may apply. In the interim however this supplemental guidance provides a minimum starting point that every CJA processing CJI can immediately put into place. Once the broader array of security controls are gleaned for a specific system, agencies can then leverage the (already implemented) controls described in this appendix as a launching pad towards full policy compliance.

The following information is organized to provide the section and section title within the CSP, along with a brief summary and background on the guidance itself. For the specific “shall” statement please go to the referenced section within the main body of the CSP.

General CJI Guidance

The following information provides CJAs guidance to maintain security compliance when setting up any system capable of sending and/or receiving CJI:

a. **3.2.9 – Local Agency Security Officer (LASO)**

It is the responsibility of the CJIS Systems Officer (CSO) to ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO) per CSP Section 3.2.2(2e).

The LASO serves as the primary point of contact (POC) between the local CJA and their respective CSA CSO or Information Security Officer (ISO) who interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to information security, disseminates information security alerts and other material to their constituents, maintains information security documentation (including system configuration data), assists with Information Security audits of hardware and procedures, and keeps the CSA (i.e., CSO or ISO) informed as to any information security needs and problems.

b. 5.1.1.3 – Criminal Justice Agency User Agreements

Any CJA receiving access to CJI must enter into a signed agreement with the CSA providing the access. The agreement specifies the services and systems the agency will access. It must also specify all pertinent governance policies to which the agency must adhere.

c. 5.1.3 – Secondary Dissemination

Secondary dissemination is the promulgation of CJI from a releasing agency to an authorized recipient agency that has not been previously identified in a formal information exchange agreement.

If CHRI is released to another authorized agency, that is not part of the releasing agency's primary information exchange agreement(s), the releasing agency must log such dissemination.

d. 5.2 – Security Awareness Training

Basic security awareness training is required for all personnel who have access to CJI within six months of initial assignment, and biennially thereafter. CSP Section 5.2.1.1 describes the topics that must be addressed within baseline security awareness training for all authorized personnel with access to CJI.

CSP Section 5.2.1.2 describes the topics required to be discussed for personnel that have both physical and logical access to CJI. These topics are covered in addition to the ones addressed in basic security awareness training.

CSP Section 5.2.1.3 describes topics to be covered for those personnel assigned information technology roles. Topics covered in this section are in addition to the topics addressed in Sections 5.2.1.1 and 5.2.1.2.

Note: The CSO may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.

e. 5.3 – Incident Response

CSP Section 5.3 assists agencies with response and reporting procedures for accidental and malicious computer and network attacks. The requirements within Section 5.3 will help CJAs with:

- (iii) Establishing an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and,
- (iv) Tracking, documenting, and reporting incidents to appropriate agency officials and/or authorities.

CSP Section 5.3.1 describes the requirements for reporting security events and describes the responsibilities of the FBI CJIS Division and the CSA ISO.

CSP Section 5.3.2 describes the requirements for managing security incidents, to include: incident handling and the collection of evidence.

CSP Section 5.3.3 describes the requirement for an agency to ensure general incident response roles responsibilities are included as part of required security awareness training.

CSP Section 5.3.4 describes the requirement for an agency to track and document information system security incidents on an ongoing basis.

Note 1: CSA ISOs serve as the POC on security-related issues for their respective agencies and must ensure LASOs institute the CSA incident response reporting procedures at the local level. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.

Note 2: CSP Appendix F contains a sample incident notification letter for use when communicating the details of an incident to the FBI CJIS ISO.

f. 5.4 – Auditing and Accountability

CSP Section 5.4 assists agencies in assessing the inventory of components that compose their information systems to determine which security controls are applicable to the various components and implement required audit and accountability controls.

CSP Section 5.4.1 describes the required parameters for agencies to generate audit records and content for defined events and periodically review and update the list of agency-defined auditable events.

CSP Section 5.4.2 describes the requirement for agencies to provide alerts to appropriate agency officials in the event of an audit processing failure, such as software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

CSP Section 5.4.3 describes the requirements for audit review/analysis frequency and to designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions.

CSP Section 5.4.4 describes the requirement to establish information system time stamp parameters for use in audit record generation.

CSP Section 5.4.5 describes the requirement to protect audit information and audit tools from modification, deletion and unauthorized access.

CSP Section 5.4.6 describes the requirement for an agency to retain audit records for at least one (1) year.

Note: The agency will continue to retain audit records for longer than one (1) year until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes - for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.

CSP Section 5.4.7 describes the requirements for logging National Crime Information Center (NCIC) and Interstate Identification Index (III) transactions. A log must be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log will clearly identify both the operator and the authorized receiving agency. III logs must also clearly identify the requester and the secondary recipient.

The identification on the log will take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one (1) year retention period.

g. 5.8 – Media Protection

CJIS Security Policy Section 5.8 assists agencies to document and implement media protection policy and procedures required to ensure that access to digital and physical media in all forms is restricted to authorized individuals for securely handling, transporting and storing media.

“Digital media” is electronic storage media, such as memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card. “Physical media” refers to CJI in physical form, e.g. printed documents, printed imagery, etc.

CSP Section 5.8.1 describes the requirement for agencies to securely store digital and physical media within physically secure locations or controlled areas and restrict access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data must be encrypted per CSP Section 5.10.1.2.

CSP Section 5.8.2 describes the requirements for agencies to protect and control both digital and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel. The agency is responsible for implementing controls to protect electronic media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in CSP Section 5.10.1.2, is the optimal control; however, if encryption of the data isn’t possible then each agency must institute other controls to ensure the security of the data.

CSP Section 5.8.3 describes the requirements for agencies to maintain written documentation of the steps taken to sanitize or destroy digital media. Agencies must sanitize (electronically overwrite the data at least three times) or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. This sanitization or destruction needs to be witnessed or carried out only by authorized personnel. Inoperable electronic media must be destroyed (cut up, shredded, etc.).

CSP Section 5.8.4 describes the requirements for physical media to be securely disposed of when no longer required, using established formal procedures. Physical media must be destroyed by shredding or incineration. This disposal or destruction needs to be witnessed or carried out only by authorized personnel.

h. 5.9 Physical Protection

CSP Section 5.9 explains the physical protection policy and procedures that are required to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

CSP Section 5.9.1 details the requirements for establishing a Physically Secure Location - a facility, a police vehicle, an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. Sections 5.9.1.1 – 5.9.1.8 describe the physical control requirements that must be implemented in order to establish a physically secure location.

CSP Section 5.9.2 details the requirements for establishing a Controlled Area. The controlled area is an area, a room, or a storage container established for the purpose of day-to-day CJI access, storage, or processing in the event an agency is unable to meet all of the controls required for establishing a physically secure location. Access to the controlled area needs to be restricted to only authorized personnel whenever CJI is processed. The CJI material needs to be locked away when unattended to prevent unauthorized and unintentional access. Additionally, the encryption standards of CSP Section 5.10.1.2 apply to the electronic storage (i.e. data “at rest”) of CJI.

i. 5.10 – System and Communications Protection and Information Integrity

CSP Section 5.10 explains the technical safeguards ranging from boundary and transmission protection to security an agency’s virtualized environment.

CSP Section 5.10.1.2 details the requirements for the encryption of CJI whether in transit or at rest. FIPS 140-2 certification is required when CJI is in transit outside a physically secure location. When at rest outside a physically secure location, encryption methods can use Advanced Encryption Standard (AES) at 256 bit strength or a FIPS 140-2 certified method.

CSP Section 5.10.3 explains the use of virtualization and partitioning when processing CJI in a virtual environment. A virtualized environment can be configured such that those parts of the system which process CJI are either physically or virtually separated from those that do not.

CSP Section 5.10.4 explains system and information integrity policy and procedures. This includes areas such as patch management, malicious code protection, and spam and spyware protection.

j. 5.11 – Formal Audits

CSP Section 5.11 explains the formal audit process to help agencies understand the audit procedures.

CSP Section 5.11.1 details the requirements for compliance and security audits by the FBI CJIS Division. The FBI CJIS Division is authorized to conduct audits, once every three (3) years as a minimum, to assess agency compliance with applicable statutes, regulations and policies.

The CJIS Audit Unit (CAU) will conduct triennial audits of each CSA in order to verify compliance with applicable statutes, regulations and policies. This audit includes a sample of Criminal Justice Agency (CJA) and NCJAs, in coordination with the SIB.

Note 1: Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies.

Note 2: The FBI CJIS Division has the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

CSP Section 5.11.2 describes the requirements for the CSA to triennially audit all CJAs and NCJAs with direct access to the state system, establish a process to periodically audit all NCJAs with access to CJI, establish the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

CSP Section 5.11.3 describes the requirement that all agencies with access to CJI must permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team, appointed by the APB, will include at least one

representative of the CJIS Division. All results of the inquiry and audit will be reported to the APB with appropriate recommendations.

k. 5.12 – Personnel Security

CSP Section 5.12 provides agencies the security terms and requirements as they apply to all personnel who have unescorted access to unencrypted CJI, including individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

CSP Section 5.12.1 details the minimum screening requirements for all individuals requiring unescorted access to unencrypted CJI.

CSP Section 5.12.2 describes the requirement for an agency to immediately terminate CJI access for an individual upon termination of employment.

CSP Section 5.12.3 describes the requirement for an agency to review CJI access authorizations and initiate appropriate actions (such as closing and establishing accounts and changing system access authorizations) whenever personnel are reassigned or transferred to other positions within the agency.

CSP Section 5.12.4 describes the requirement for an agency to employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

l. 5.13 – Mobile Devices

When access to CJI using mobile devices such as laptops, smartphones, and tablets is authorized, CSP Section 5.13 explains the controls required to manage those devices to ensure the information remains protected.

The following scenarios are intended to help the reader identify areas within the CSP that CJAs may often come across. Each scenario should be reviewed for applicability in conjunction with the above “General CJI Guidance” section. The specific requirements found with the CSP are not shown; however specific sections are referenced along with a requirements summary.

Hard Copy CJI Storage and Accessibility

When CJI is received in hard copy and the agency stores the paper within a locked file cabinet, the CJA should, in addition to the “General CJI Guidance”, focus on compliance with policy section:

a. 4.2.4 – Storage

When storing CJI, appropriate administrative, technical, and physical safeguards must be implemented to ensure the security and confidentiality of the information.

Electronic CJI Storage and Accessibility – Controlled Area

When an agency creates an electronic copy of CJI (e.g. scanning a document or creation of a spreadsheet) and subsequently stores this static CJI on either a local hard drive or shared network drive in a controlled area for indirect access by Authorized Recipients, the agency should, in addition to the “General CJI Guidance”, focus on compliance with policy section:

a. 5.5.2.4 (3) – Access Control Mechanisms – Encryption

CSP Section 5.5.2.4 item 3, Encryption – This describes the requirement for utilizing encryption as the primary access control mechanism which is necessary in this

situation. Encrypted information can only be read by personnel possessing the appropriate cryptographic key (e.g., passphrase) to decrypt. Refer to Section 5.10.1.2 for specific encryption requirements.

Electronic CJI Storage and Accessibility – Physically Secure Location

When an agency receives or creates an electronic copy of CJI and subsequently stores this CJI within a Records Management System (RMS), located within a physically secure location that may be queried by Authorized Recipients, the agency should, in addition to the “General CJI Guidance”, focus on compliance with policy sections:

a. **5.5 – Access Control**

CSP Section 5.5 describes the requirements and parameters for utilizing access control mechanisms for restricting CJI access (such as the reading, writing, processing and transmission of CJIS information) and the modification of information systems, applications, services and communication configurations allowing access to CJI to only authorized personnel.

b. **5.6 – Identification and Authentication**

CSP Section 5.6 describes the requirements and parameters agencies must implement to validate and authenticate the identity of information system users and processes acting on behalf of users the identities prior to granting access to CJI or agency information systems/services that process CJI.

c. **5.7 – Configuration Management**

CSP Section 5.7 describes the requirements for implementing access restrictions that will only permit authorized and qualified individuals access to information system components for purposes of initiating changes, including upgrades, and modifications.

CSP Section 5.7.1 describes the requirements for implementing the concept of least privilege (5.7.1.1) and for developing and maintaining network diagrams (5.7.1.2) that detail how the RMS is interconnected and protected within the network. See Appendix C for sample network diagrams.

CSP Section 5.7.2 details the requirement for agencies to protect the system documentation from unauthorized access consistent with the provisions described in Section 5.5 Access Control.

d. **5.10 – System and Communications Protection and Information Integrity**

CSP Section 5.10 details the requirements for network infrastructures within physically secure locations through establishment of system and communication boundary and transmission protection safeguards that assist in securing an agency’s environment, even when virtualized. In addition, this section describes the requirements for providing the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information for applications, services, and information systems.

Use Case Scenarios

1. Indirect Access to Criminal Justice Information (CJI) Stored on a Network Server

A county court scans hard copy case documents containing CJI into an electronic format. The documents are placed on a network server which is located in a secure data center within the court offices. The data center meets all the requirements to be labeled a physically secure location as defined in Section 5.9.1 of the CSP.

Keeping in mind the scenario as described, an authorized user needs access to case documents. This user is not located in the secure data center and will have to use remote access to access the file. The user is therefore required to provide identification and authentication credentials to prove they are an authorized user. To access the documents, the user is prompted to enter their unique username and password. Because the documents reside on a system with indirect access to CJI (does not allow the user to query a state or national criminal record repository), AA is not required for access to the documents.

NOTE: If the Authorized User has direct access to CJI (the ability to query a state or national criminal record repository) in the above scenario, AA would be required.

2. Encryption for Data at Rest (Exemption for FIPS 140-2 Certified Encryption)

A county court scans hard copy case documents containing CJI in an electronic format. The documents are placed on a network server which is not located in a secure data center. Because the data center does not meet the requirements of a physically secure location, as defined in Section 5.9.1 of the CSP, the files, at rest (in storage) on the server, are required to be encrypted.

To prevent unauthorized access, the IT staff has decided to encrypt the entire folder that contains the files. They will use a product that provides an advanced encryption standard (AES) algorithm at 256 bit strength to comply with the CSP and employ a CSP compliant passphrase to lock the folder's encryption. When an authorized user needs to access to the case documents, they access the folder on the server and are prompted to enter the designated passphrase to decrypt (unlock) the folder. The user can then access all files within the folder. Additionally, because the documents reside on a system with indirect access to CJI (does not allow the user to query a state or national criminal record repository), AA is not required for access to the documents.

NOTE: Whenever authorized personnel no longer require access to the encrypted folder, the passphrase must be changed to prevent future access by that user.

Appendix XVII – System Requirements Matrix



**Food Service Management
System Requirements Matrix**

RFP Offeror Instructions

This workbook contains Functional, Proposal, and Technological Requirements for the system desired by Cook County. The response codes below should be used by responders to indicate the fit of their solution to the requirements specified in this workbook.
This template must be completed and submitted as an MS Excel file as part of the response to this RFP.

Responses	Definition
Response Code: How will this Technical Requirement be met by your solution?	Please note that all requirements must be met by one of the possible solution options described below.
	Indicate how the requirement will be met by selecting either: Requirement Met, Requirement Not Met, Requirement Met by Third Party Product:
	Y= Requirement Met
	N = Requirement Not Met
	T= Third Party Product – The requirement will be met by commercially available third-party software or hardware assets and is included in this proposal. Note: In the Offeror Response column, indicate the name of the proposed third-party software vendor and proposed components and indicate its compliance to Cook County's technology or architecture standards.
	NA - Not applicable / Not Supported - Vendor does not have this service/capability/offering
Offeror Response Comments & Response Narratives	Provide comments as necessary in regards to specific requirements using this response template. To provide more extensive details and documentation regarding the approach for meeting a requirement, or combination of requirements, or overall Technical area, use a text/Word document and provide a reference to the appropriate RFP Req. #(s).
Description of Other Fields	RFP Req #: Identification of where these Requirements can be found in the RFP.

Food Service Management System Requirements and Overview			
Please provide a response code and offeror response for each requirement.			
RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
Detainee Meal Service			
2.1.1	Verify that software provided by the Proposer shall enable CCSO to electronically generate meal orders for all three (3) meals.		
2.1.1	Verify that software provided by the Proposer shall enable CCSO to electronically submit completed meal order forms containing the total number of detainee meals to be served for the applicable meal—breakfast, lunch, or dinner—and the number of each and any therapeutic/specialty diet meals to be served within those totals to the Proposer three (3) times per day.		
2.1.1	Provide a computerized daily meal order report that shall include, but not be limited, to the following information: date and time meal order was placed; type of meals ordered; number of meals ordered; number of meals changed; number of meals served; number of meals returned; location for which the meals were ordered.		
2.1.2	Acknowledge that all detainee meals will be prepared on-site in the CCDOC Central Kitchen except in the event of an emergency and/or if the CCDOC Central Kitchen is unavailable.		
2.1.2	Acknowledge that approval must be obtained from the CCSO prior to preparing any meals off-site in the event of an emergency and/or if the CCDOC Central Kitchen is unavailable.		
2.1.2	Acknowledge that all detainee meals will conform to the guidelines and standards for food quality and preparation set forth in the Food Service RFP.		
2.1.3	Verify that detainee meals shall be delivered according to the food service delivery schedule established by the CCSO		
2.1.3	Acknowledge that reliable and timely delivery of meals to CCDOC delivery locations at a reasonable interval for breakfast, lunch, and dinner is essential to meet detainee daily diet needs and maintain compliance with food safety standards.		
2.1.3	Acknowledge understanding that all food service must comply with the Illinois Jail Standards, 20 Ill. Adm. Code 701.110.		
2.1.3	Acknowledge that per the Illinois Jail Standards, no more than fourteen (14) hours may elapse between the evening meal and the next morning's breakfast.		
2.1.3	Describe how Proposer shall place prepared meals into insulated food carts provided by the CCSO, loaded to maximize efficient transportation and distribution of meals, according to the CCSO's food service delivery schedule.		
2.1.3	Describe how Proposer shall position the loaded food carts in the CCDOC designated area within Central Kitchen. The CCSO will pick up food carts from the designated area and deliver to all delivery locations.		
2.1.3	Describe how Proposer shall package breakfast and lunch meals in a single, sealed, transparent containers that protect food products from contamination by insects or foreign substances.		
2.1.3	Describe how Proposer shall utilize insulated compartmented trays provided by the CCSO for dinner meals.		
2.1.3	Acknowledge that it may be necessary for Proposer to provide and utilize single use packaging as directed by the CCSO.		

Food Service Management System Requirements and Overview			
<i>Please provide a response code and offeror response for each requirement.</i>			
RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
2.1.4	Acknowledge that upon award of the contract, Proposer shall strictly provide all items on the approved food service menu.		
2.1.4	Acknowledge that any menu substitutions must be submitted to the CCSO for approval at least twenty-four (24) hours in advance, and tracked and maintained for a minimum duration of ninety (90) days and must be provided upon request by regulatory authorities in the event of epidemiological investigation during foodborne illness incident or any other food safety related issues.		
2.1.4	Acknowledge all detainee menu items must be reviewed and approved by the CCSO to ensure compliance with security protocols and policies.		
2.1.5	<p>Provide healthy and nutritious meals with total daily caloric intake of 2,300-2,500 kcal that are low fat, low sodium, appropriate for the detainee population, and meet following requirements:</p> <ul style="list-style-type: none"> - No pork product or pork derivative may be on the menu. - No seafood product or seafood derivative may be on the menu. - The same type of meat shall not be served more than once a week. - No alcohol or alcohol derivative may be used in the preparation of meals on the menu. - Milk shall be served a minimum of one (1) time per day in individual 8-ounce portions. - A minimum 10% fruit juice drink shall be served with the breakfast meal, fortified with Vitamin C, supplied in individual 4-ounce portions. A fruit drink (8 ounces) shall be served with the lunch meal. - Jelly shall be provided at all breakfast meals except when syrup is required. - Wheat bread must be served two meals per day; the third meal may be white bread. - When donuts, dinner rolls, buns or cornbread appears on the menu additional bread is not required. - One (1) starch item, such as potatoes, rice, and/or noodles. Portion size: 1 cup. - One (1) vegetable item, such as California blend, oriental blend, broccoli, and/or greens. Portion size: ½ cup. - One (1) dessert item, such as fresh fruit, cake, cobblers, ice cream, and/or pie. Portion size: one (1) each. - Two (2) types of bread, such as wheat, white, rye, and/or pumpernickel. Portion size: two (2) slices. - Self-serve Beverages, including all of the following: Coffee, tea, milk, fruit drink, assorted soft drinks and water. - Self-serve condiments, such as salt, pepper, ketchup, mustard, mayonnaise, relish and hot sauce (ketchup, French, etc.) but not on consecutive days. - Fruit options may be restricted at CCSO's direction based on considerations related to institutional safety. - Red pepper bologna is prohibited from use by the Proposer. 		
2.1.5	Provide proposed menus based on the examples in Appendix IV of the Food Service RFP that include the following nutritional information for all detainee meals: Calories (kcal); Fat (gm); Percent of calories from fat (%); Saturated Fat (gm); Percent of calories from saturated fat (%); Protein (gm); Carbohydrate (gm); Cholesterol (mg); and Sodium (mg).		

Food Service Management System Requirements and Overview			
<i>Please provide a response code and offeror response for each requirement.</i>			
RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
2.1.5	Acknowledge that Proposer shall not use food that has been prepared or stored in violation of any applicable Food Safety code, or regulation including Federal, State and Local Food Safety Regulations.		
2.1.6	Acknowledge that Proposer shall prepare and deliver any and all therapeutic diet meals ordered by Cook County Health and Hospitals System ("CCHHS") personnel, with the meals conforming to all dictated medical criteria and served as ordered.		
2.1.6	Amendments to prescribed medical diets included in the cost of the meal and not billed separately by Proposer.		
2.1.6	Submit copy of dietary manual and provide examples of dietary menus that include all the nutritional information required in Section 2.1.5. of the RFP.		
2.1.6	Acknowledge understanding that the following is a non-exhaustive listing of the current therapeutic diets, all of which shall be made available daily, upon request: Cholesterol/Fat Restricted/Low Salt (300 mg cholesterol, 30% Fat, 4gm NA); Dental Soft; Nutrition Support Diet with Healthy Snack; Diabetic 2400 Cal A.D.A. with Healthy Snack; 3200 Cal A.D.A. with Healthy Snack; Pregnancy with Healthy Snack; Full Liquid; Clear Liquid Diet; Renal Diet; Vegan; Food Allergy/Other Diets (i.e. No Lactose, No Gluten, No Peanut, etc.).		
2.1.7	Provide meals for detainees in accordance with the Religious Land Use and Institutionalized Persons Act (RLUIPA), 42 U.S.C. §§ 2000cc, et seq., and comply with all other federal, state, or local laws and court decisions, at no additional fee or charge to the CCDOC.		
2.1.7	Provide certified meals for religious diets as described in Religious Diet Programs, Certified Food Components, Ch. 4-1, Food Service Manual published by the U.S. Bureau of Prisons (2011) or most recent edition.		
2.1.7	Submit examples of proposed religious diet menus that include all the nutritional information required in Section 2.1.5. of the RFP.		
2.1.8	Acknowledge that Proposer shall prepare holiday menus for meals to be served on the following holidays: New Year's Day, July 4th, Thanksgiving and Christmas, and either prepare holiday menus on Easter, Memorial Day, and Labor Day or in the alternative provide one (1) monthly Saturday or Sunday Dinner Meal that includes a whole meal meat (e.g., Fried Chicken, Roast Beef or Turkey-Ham), for each month that does not include a mandatory Holiday Menu.		
2.1.8	Acknowledge that all holiday menus shall be submitted at least one (1) month in advance for approval by the CCSO.		
2.1.8	Acknowledge that therapeutic diet meals shall be adjusted to reflect the holiday menus where feasible.		
2.1.8	Acknowledge that holiday meals shall be the same cost per meal as a regular diet meal and that holiday menu portions shall equal or exceed those provided by non-holiday menus.		
2.1.8	Submit examples of proposed holiday menus that include all the nutritional information required in Section 2.1.5. of the RFP.		

Food Service Management System Requirements and Overview			
<i>Please provide a response code and offeror response for each requirement.</i>			
RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
Court Services Department (CSD) Meal Service			
2.2	Provide CSD meals consisting of: two (2) sandwiches, each of which shall contain two (2) slices of bread and either three (3) ounces of meat or two (2) ounces of meat and two (2) ounces of cheese; two (2) condiment packets; and one eight (8) ounce fruit drink.		
2.2	Acknowledge that Proposer shall provide a meal for each detainee in CSD Criminal Courts Building lock-up, one (1) time per day, seven (7) days per week and to the specified CSD courthouses one (1) time per day on Monday and Wednesday.		
2.2	Verify that software provided by the Proposer shall enable CCSO to provide the Proposer with the requested CSD meal order count daily for all CSD courthouses.		
2.2	Acknowledge that all CSD meals shall be placed in the CCDOC designated area within Central Kitchen pursuant to the meal order count and meal delivery times provided by the CCDOC.		

Food Service Management System Requirements and Overview			
<i>Please provide a response code and offeror response for each requirement.</i>			
RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
Officer's Dining Room (ODR) Meal Service			
2.3	Provide food services for CCSO staff and authorized visitors in all designated ODR's, which are open 24/7 to accommodate all shifts.		
2.3	<p>Provide proposed ODR menus for meals that meet the following minimum requirements:</p> <ul style="list-style-type: none"> - One (1) hot entrée. Entrees must contain at least 3 oz. of meat; one entrée item must be a whole meat. Portion size: 1 serving. Meat patties and casseroles shall be served no more than two (2) times per week. - Two (2) types of sandwiches. Each sandwich must contain at least three (3) ounces of meat, fish or poultry. - One (1) type of grill item, such as hot dogs (jumbo only), polish sausage, hamburger, grilled cheese, etc. Portion size: 2 grilled cheese, all others one item. - Made to Order Salads. The following items are required, at all times for Made-to-Order salads: Pasta Salad, Coleslaw, Plain Tuna, Mixed Salad Greens, Fresh Spinach, Tomatoes, Broccoli, Green Peppers, Cauliflower, Onions, Carrots, Cucumbers, Cheese, Croutons, and four (4) types of Salad Dressing. - A pre-packaged nutrient-dense salad is allowed in addition to the made to order salads, with a choice of at least four (4) types of salad dressing. - One (1) starch item, such as potatoes, rice, and/or noodles. Portion size: 1 cup. - One (1) vegetable item, such as California blend, oriental blend, broccoli, and/or greens. Portion size: ½ cup. - One (1) dessert item, such as fresh fruit, cake, cobblers, ice cream, and/or pie. Portion size: one (1) each. - Two (2) types of bread, such as wheat, white, rye, and/or pumpernickel. Portion size: two (2) slices. - Self-serve Beverages, including all of the following: Coffee, tea, milk, fruit drink, assorted soft drinks and water. - Self-serve condiments, such as salt, pepper, ketchup, mustard, mayonnaise, relish and hot sauce. 		
2.3	Acknowledge that menu plans shall be posted in the ODR at least one week in advance.		
2.3	Acknowledge that menu revisions shall be submitted to the CCSO for approval at least two (2) weeks before planned implementation and menu substitutions shall be submitted for approval at least twenty-four (24) hours in advance.		
2.3	Acknowledge that menu substitutions shall be tracked and maintained for a minimum duration of ninety (90) days and must be provided upon request by regulatory authorities in an event of epidemiological investigation during foodborne illness incident or any other food safety related issues.		

Food Service Management System Requirements and Overview			
<i>Please provide a response code and offeror response for each requirement.</i>			
RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
Food Service Staffing Requirements			
2.4	Acknowledge that any person working with or around food shall be trained in food safety and sanitation and shall possess and maintain a Food Handler Certification, as required by the Illinois Department of Public Health Food Service Sanitation Code (77 Ill. Adm. Code 750).		
2.4	Provide qualified civilian staff at the CCDOC Central Kitchen and ODR locations that shall, in conjunction with assigned detainee workers, prepare all detainee and CSD meals in the CCDOC Central Kitchen.		
2.4	Acknowledge that detainees are strictly prohibited from preparing any food to be served in conjunction with ODR meals.		
2.4	Describe the level of support and supervision required during the food service preparation process, acknowledging that the level of support and supervision such as detainee workers and security supervision may be subject to fluctuation as a result of external conditions beyond the control of the CCSO.		
2.4	Describe the hiring practices and training procedures for employees assigned to service this contract.		
2.4	Acknowledge that Proposer training must be documented, and the records made available for review by the CCSO and Cook County upon request.		
2.4	Acknowledge that Proposer's on-site employees shall be required to complete any and all applicable CCSO civilian training or orientation prior to work assignment.		
2.4.1	Provide direct supervision to ensure regulatory food safety and sanitation standards are met, and equipment is utilized according to manufacturer specifications.		
2.4.1	Provide adequate supervision of all food service staff, including detainee workers, at all times and in all areas of food service operation, including a sufficient number of Managers with Food Safety and Sanitation Manager Certifications (FSSMC) or Food Handlers to supervise each post.		
2.4.1	Acknowledge that supervisory staff shall be in attendance whenever the facilities are in operation and shall be assigned exclusively to the performance of Proposer's obligations under this contract to assure quality performance.		
2.4.1	Acknowledge that any change in supervisory personnel must be cleared in advance and approved by the CCSO.		
2.4.1	Provide proposed operational policies and procedures (i.e. Sanitation, HACCP, training, tool security and inventory, etc.) that will be followed by its employees assigned to service this contract.		
2.4.2	Provide a sufficient number of non-management employees to meet all requirements of this food service contract, including proper direct supervision of detainee workers.		

Food Service Management System Requirements and Overview			
<i>Please provide a response code and offeror response for each requirement.</i>			
RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
2.4.2	Acknowledge that Proposer shall comply with the following minimum standards as it related to non-management employee staffing: - CCDOC Central Kitchen Food Line: One (1) Proposer non-management employee shall be assigned to monitor each food line in the CCDOC Central Kitchen while in operation. - CCDOC Central Kitchen Sandwich Production: At least two (2) Proposer non-management employees shall be assigned to supervise sandwich production. - CCDOC Central Kitchen Tray Wash Area: No less than two (2) Proposer non-management employees shall be present to supervise tray washing operations. - CCDOC ODR Locations: Proposer shall ensure all ODR non-management employees possess valid food handler certification within thirty (30) days upon employment and subsequently renew thereafter according to the expiration date. ODR must be operational 24 hours per day, 7 days per week. No detainee workers shall be assigned to work in ODR locations.		
2.4.3	Provide a complete staffing plan with their proposal, which includes: the total number of management staff, and non-management staff by location; a daily staff (managers and employees) assignment schedule for each shift and work group (based on regular days off); an organizational chart; and job descriptions for all positions.		
2.4.3	Acknowledge that Proposer shall keep a complete roster of all employees assigned to perform services under the contract, that includes both filled positions with staff names and start date and vacant positions with date vacated, and provide a current, electronic copy of same to the CCSO monthly.		
2.4.3	Acknowledge that Proposer shall provide timesheets for all employees, including managers, for each shift, work group and work location to the CCSO within 48 (forty-eight) hours after the close of each pay period for the duration of the contract.		
2.4.3	Acknowledge that Proposer shall maintain standard operating procedures governing the daily assignment of the work within Food Management Services under the contract. Delegation of authority within Food Management Services will be clearly defined in the standard operating procedures for the duration of the contract.		
2.4.3	Acknowledge that Proposer shall comply with all CCSO policies, procedures and directives relevant to food service operations and shall communicate these policies, procedures and directives to all Proposer employees assigned to this contract.		
2.4.3	Acknowledge that Proposer shall maintain Food Safety and Sanitation Manager and Food Handler Certificates for employees assigned to perform services under the contract and shall provide such certificates upon request from CCSO and all Regulatory Authorities.		
2.4.4	Acknowledge that Proposer's employees are required to attend applicable civilian training and/or orientation provided by the CCSO.		
2.4.4	Acknowledge that Proposer shall be responsible for providing forty (40) hours of orientation/training during the first six (6) months of assignment under the contract to all new Proposer employees		

Food Service Management System Requirements and Overview			
<i>Please provide a response code and offeror response for each requirement.</i>			
RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
2.4.4	Acknowledge that Proposer shall be responsible for ensuring ensure that all Food Service staff has access to the Illinois Food Sanitation Code and the U.S. Public Health Service Food Code.		
2.4.4	Acknowledge that Proposer shall provide annual training for its employees servicing the contract that incorporates relevant CCSO policies and procedures and any specific training necessary for Proposer employees operating equipment that includes, but is not limited to: (i) proper operation, cleaning, and sanitizing of all equipment; (ii) the inherent dangers of each piece of equipment; (iii) symptoms of equipment malfunction; and (iv) staff responsibility to immediately report all hazards, malfunctioning equipment, or unsafe conditions to their supervisors.		
2.4.4	Acknowledge that all training must be documented, and the records made available for review by the CCSO and Cook County upon request.		
2.4.5	Provide a description of all proposed detainee worker assignments and shift schedules.		
2.4.5	Acknowledge that if more than one hundred detainees are required by the Proposer, the Proposer will compensate the County, for the additional detainees, based upon current detainee payroll rates in effect at the time of the request.		
2.4.5	Acknowledge that Proposer shall be responsible for training all assigned detainee workers in the performance of their assigned tasks.		
2.4.5	Acknowledge that Proposer shall collaborate with the CCSO in the design and implementation of a Kitchen Worker Orientation Training program, that shall include, at minimum, instruction as follows: Central Kitchen Security Rules & Regulations; Food preparation and handling procedures; Sanitation and proper grooming; Energy conservation methods; Recycling; Handling waste and properly recycling non-waste materials during the preparation and service of meals; and any other area the Proposer deems necessary for the performance of this contract.		
2.4.5	Acknowledge that Proposer must comply with the Illinois Food Handling Regulation Enforcement Act in utilizing detainee workers. See 410 ILCS 625.		
2.4.5	Acknowledge that Proposer shall be responsible for ensuring that all detainee workers acquire food handling certifications during the course of each of their food service assignments at no cost to the CCSO or County.		
2.4.6	Submit a detailed description of the uniforms proposed to be worn by on-site Proposer employees. Employee uniforms shall be black or white in color		
2.4.6	Acknowledge that all Proposer employee uniform costs shall be borne by the Proposer.		
2.4.6	Acknowledge that Proposer shall provide laundry services for detainee uniforms to ensure clean uniforms on a daily basis for detainee workers.		
2.4.6	Acknowledge that Proposer shall provide detainee workers with hair net/hats, beard guards, plastic/cloth aprons, plastic gloves, rubber gloves and rubber boots for tray washing.		
2.4.6	No employee or detainee uniforms or other items listed in Section 2.4.6 may be considered part of the Cost per Meal.		

Food Service Management System Requirements and Overview			
<i>Please provide a response code and offeror response for each requirement.</i>			
RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
Key Personnel			
2.5	Submit a current organizational chart of its key positions including, but not limited to, executive and management staff with names and titles.		
2.5	Submit Qualifications of Key Personnel, including resumes reflecting certifications and experience working within food service systems for institutions of similar scale to CCDOC, if applicable.		
2.5	Provide a Food Service Director, dedicated solely to this contract, with at least three (3) years of experience in the field of large institutional food service management.		
2.5	Acknowledge that Proposer shall not remove or reassign the Food Service Director from the CCDOC for a minimum period of one (1) year without the approval of the CCSO, unless removal is requested by the CCSO.		
2.5	Provide enough Food Service Managers with all requisite food service and public health certifications under federal, state, county and local law for food service operation, to ensure that at least one (1) Food Service Manager is on-site at all times during food preparation, per the Illinois Administrative Code.		
2.5	Acknowledge that a licensed Food Service Manager is present during all food preparation for both Detainee/CSD meals and ODR meals, as food served in ODR must be prepared separately from food prepared for Detainee and CSD Meals.		
2.5	Provide at least one (1) full time, on-site Dietician registered and licensed by the State of Illinois.		
2.5	Acknowledge that the Dietician shall not work in the capacity of the Food Service Director or Food Service Manager.		
2.5	Acknowledge that the Dietician's responsibilities shall include, but not be limited to, the following: <ul style="list-style-type: none"> - Manage the daily provision of therapeutic diets. - Help resolve problems related to therapeutic diets. - Monitor the Hazard Analysis and Critical Control Points ("HAACP") program, document related problems and solutions. - Monitor Quality Assurance and Sanitation, document related problems and solutions. - Generate and approve regular and therapeutic menus for use at CCDOC. - Conduct in-service training for the Proposer's employees and for detainees who participate in the provision of services as detailed herein. - Work with the CCSO, as well as CCHHS/Cermak Health Services to resolve problems related to the food service operation. 		

Food Service Management System Requirements and Overview			
<i>Please provide a response code and offeror response for each requirement.</i>			
RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
Food Service Contingency Plan			
2.6	Submit a Contingency Plan for providing uninterrupted food services in the event of lockdowns, strikes by Proposer's employees, riots, fire, power failure or other catastrophic events that may curtail or impact the normal operations of the CCDOC		
2.6	<p>The Contingency Plan and any future amendments shall include, but not be limited to the following:</p> <ul style="list-style-type: none"> - Step by step outline of Proposer's plan of action in the event of a catastrophic occurrence, listing (when appropriate) names, phone numbers and addresses of contacts. - Designation of offsite locations that comply with local Department of Health and/or Federal Food Safety Codes for food preparation and storage. - Alternative staffing plans. - Any other information Proposer deems necessary to demonstrate its capability to provide uninterrupted service in the event of a catastrophic occurrence. 		

Food Service Management System Requirements and Overview			
<i>Please provide a response code and offeror response for each requirement.</i>			
RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
Facilities and Equipment			
2.7.1	Acknowledge that CCDOC facilities made available to the Proposer under the contract may not be used for any operations unrelated to the performance and delivery of food services under the contract.		
2.7.2	Acknowledge that Proposer is responsible for properly handling pre-cleaning of food trays, etc., to ensure the drains stay clean and free of debris and that Proposer shall be responsible for any damage to plumbing systems that is due to Proposer's neglect.		
2.7.2	Acknowledge that Proposer shall be responsible for the cost of repairs due to negligence or abuse by the Proposer's employees or detainee workers due to inadequate supervision or training.		
2.7.2	Acknowledge that Proposer shall define and document the need for building repairs by initiating a work order through the CCSO's established procedures.		
2.7.3	Acknowledge that all CCSO-owned food service equipment in the CCDOC Central Kitchen, ODR Kitchen, and all other designated locations provided by the CCSO for use by Proposer during the term of the contract shall remain the property of the CCSO.		
2.7.3	Acknowledge that upon award of the contract, Proposer and the CCSO shall jointly conduct an initial inventory of food service equipment provided by the CCSO, and that unless otherwise expressly noted, it shall be presumed that the Proposer accepts the equipment as initially inventoried, as in good working order, and sufficient for the purpose of performing the contract.		
2.7.3	Acknowledge that, following the initial inventory of equipment, Proposer and the CCSO shall conduct a joint inventory of equipment semi-annually, not later than June 30 and December 31 for each year of the contract.		
2.7.3	Acknowledge that Proposer shall provide a quarterly report to the CCSO on the status and condition of the equipment that shall state with specificity the Proposer's recommendations for equipment maintenance and replacement.		
2.7.3	Acknowledge that Proposer shall be responsible for maintaining records of all equipment added, replaced and/or removed from the initial inventory that shall be made available to the CCSO upon request and shall include sufficient information to document the following: - Description of the equipment including the manufacturer's name, make and model of the equipment, manufacturer's identification number, useful life of the equipment, and the date the equipment was placed into service. - The date(s) the equipment received preventative maintenance and the name of the company providing preventative maintenance. - The date(s) the equipment was repaired due to malfunction or damage, a description of the malfunction or damage, and the name of the company providing repairs.		
2.7.3	Acknowledge that any equipment purchased by Proposer to aid in the increased efficiency and delivery of contract services shall meet the National Sanitation Foundation (NSF) or Underwriters Laboratories (UL) standards.		

Food Service Management System Requirements and Overview			
<i>Please provide a response code and offeror response for each requirement.</i>			
RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
2.7.3	Acknowledge that any equipment purchased by Proposer must be added to the inventory and designated as "Proposer Owned" on all inventory reports, and shall remain the property and sole responsibility of the Proposer at the end of the contract term.		
2.7.3	Acknowledge that Proposer shall be liable for the replacement and installation costs of all CCSO-owned equipment that is unaccounted for or has unaccounted for damage in the closing inventory.		
2.7.4	Acknowledge that Proposer shall be responsible for providing, at its own expense, general maintenance to all dietary areas occupied and used by the Proposer.		
2.7.4	Acknowledge that Proposer shall be responsible for providing, at its own expense, proper preventative maintenance pursuant to manufacturer instructions and repair of the following CCSO-owned food service equipment for the life of the contract: All kitchen equipment, including exhaust systems, hoods, kitchen fire protection equipment, kettles, ovens, dishwashers, food service carts, and conveyor equipment and all electrical, heating and refrigeration units, including the compressors, that are used to service the CCDOC Central Kitchen, ODR, and within the preparation, service, receiving and storage areas.		
2.7.5	Acknowledge that Proposer shall provide all supplies and small wares used in performance of the contract, including, without limitation: disposable eating utensils for each meal except authorized sack lunches; serving utensils; pots and pans; paper products, including napkins; plastic wrapping materials; and service ware items, such as disposable trays.		
2.7.5	Acknowledge that only supplies that comply with Cook County recycling and environmental ordinances shall be used.		
2.7.5	Acknowledge that proposer shall provide all commodities, including foodstuffs, dry goods, canned foods, frozen foods, cereal, spices and the like, and shall draw all commodities in a first in, first out basis, and all non-perishable food items will be marked with the color identifying the quarter it was received to ensure proper stock rotation.		
2.7.5	Acknowledge that Proposer shall be required to review the specifications and utilization of such supplies with the CCSO and obtain approval before such supplies may be employed at the CCDOC.		

Food Service Management System Requirements and Overview			
<i>Please provide a response code and offeror response for each requirement.</i>			
RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
Sanitation and Pest Control			
2.8.1	Acknowledge that Proposer shall be responsible for cleaning and housekeeping in the food preparation, CCDOC Central Kitchen, ODRs, and all associated washroom and locker-rooms, service and storage areas, elevators, and will keep such areas in a clean and sanitary condition, and in conformity with all applicable federal, state and local regulations and requirements.		
2.8.1	Acknowledge that Proposer shall be responsible for providing cleaning, janitorial and housekeeping materials, all of which must comply with the CCSO's rules, regulations, policies and procedures, and with County, State and Federal EPA and food service laws and regulations.		
2.8.1	Acknowledge that Proposer shall establish hazardous chemical logs and comply with all applicable CCSO rules, regulations, policies and procedures concerning the use, storage and handling of hazardous substances.		
2.8.2	Develop and maintain an effective program for extermination and control of vermin and rodents, which includes pest control services to be performed on a weekly basis for the entire CCDOC Central Kitchen, ODR, and any and all food service and dining areas.		
2.8.2	Acknowledge that Proposer shall coordinate its pest control program with the vermin control programs conducted by the CCSO's contracted pest control vendors.		
Cost Accounting System & Reporting			
2.9	Verify that Proposer shall provide a computerized Food Service Management Cost Accounting System ("Accounting System") that shall record and itemize all meals ordered, prepared, and delivered by the Proposer for the term of the contract.		
2.9	Acknowledge that the CCSO retains sole ownership of the CCSO's data contained within the Proposer's proposed Accounting System.		
2.9	Acknowledge that the CCSO's data is proprietary and confidential and shall not be used by the awardee for any purpose other than what is required by this RFP.		
2.9	Acknowledge that maintenance of all provided software and hardware shall be the responsibility of the Proposer for the duration of the contract terms, including renewal years.		
2.9	Address in the Technical Proposal how Proposer's Accounting System will electronically track all meal ordering, daily meal order reports, billing, inventory, small wares, supplies, uniforms, and food service operation activity up to and including menu preparation and compliance, recipe preparation, food production, equipment maintenance and repair, and other budgetary activity.		

Food Service Management System Requirements and Overview			
<i>Please provide a response code and offeror response for each requirement.</i>			
RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
2.9	<p>Address in the Technical Proposal how Proposer's Accounting System will interface with the CCSO Jail Management System and any subsequent versions for the life of the contract, when the interface must include, but is not limited to, continuous synchronization of data concerning CCDOC detainee meal specifications with individual booking profiles and the data must be transferred in the following format:</p> <ul style="list-style-type: none"> - Booking Id (nvarchar(100)) - Inmate ID (nvarchar(100)) - Inmate Name (nvarchar(100)) - Bed assignment (nvarchar(100)) - Meal plan Category (nvarchar(100)) <ul style="list-style-type: none"> i. Administrative ii. Religious iii. Regular iv. Medical v. Work Detail Supplied - Meal Plan Description (nvarchar(100)) - Effective Date (Datetime) - End Date (datetime) - Approved By (nvarchar(100)) - Date booked (datetime) - Division Assigned (nvarchar(100)) - Tier Assigned(nvarchar(100)) 		
2.9	Address in the Technical Proposal how Proposer's Accounting System will electronically track all ODR meals, including how Proposer will register staff meal service by scanning proximity cards, including 37-bit HID cards, sustain an integration between the CCSO's employee proximity card table and Proposer software, and integrate the Sheriff's Office's active employee tables.		
2.9	Verify that Proposer's system will be able to accept 37 BIT HID proximity cards, account for staffing status changes and custom/ad hoc reporting as needed, have data sent back to CCSO BOIT with employee purchasing information, allow CCSO BOIT to run custom/ad hoc reports, and provide daily automated reports to the CCSO BOIT.		
2.9	Address in the Technical Proposal how Proposer's Accounting System will record and track each staff meal ordered and delivered in CCDOC ODRs, including the individual employee that scanned for each meal, the date and time of the proximity scan, and all other data elements as directed by the CCSO.		
2.9	Address in the Technical Proposal how Proposer's Accounting System will enable to CCSO to determine the cost per meal under the contract, broken out by the type of meal and the recipient.		

Food Service Management System Requirements and Overview			
<i>Please provide a response code and offeror response for each requirement.</i>			
RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
2.9	Address in the Technical Proposal how Proposer's Accounting System will ensure safeguards for computer hardware, software, and data access so as to comply with the IT Special Conditions set out in Appendix XIV of the RFP.		
2.9	Address in the Technical Proposal how Proposer's Accounting System will provide continued operation with minimum interruption as well as backup of all data in the event of server error(s).		
2.9	Address in the Technical Proposal how Proposer's Accounting System will		
2.9	Address in the Technical Proposal how Proposer's Accounting System will enable to CCSO to directly access all data stored in Proposer's Accounting System, grant CCSO BOIT will be direct access, via VPN or through integrations (API,SFTP, FTPS), enable the CCSO to query, or have Proposer create custom queries and send data back to CCSO BOIT on a schedule (automated jobs) based on operational needs.		
2.9	Address in the Technical Proposal how Proposer will supply, install, and maintain, at no cost to the County, all necessary technology, equipment, including on-site computers/workstations, server, wiring, and any other technology and/or resources required for operation of Proposer's Accounting System for all food service locations.		
2.9	Verify that Proposer's technology is adaptable to all computer software, wiring, programming and hardware upgrades as directed by the CCSO and meets the following basic requirements: Processor - Intel 8th Generation Core i7 Quad Core Minimum; Memory - 16GB; Chipset - Intel Q270 Chipset; Graphic Options - Integrated Intel HD Graphics 610/630 (Intel 8th Generation); Operating System - Windows 10 Enterprise 64bit; Networking - 1 Gigabyte minimum		

Food Service Management System Requirements and Overview			
<i>Please provide a response code and offeror response for each requirement.</i>			
RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
2.9.1	<p>Verify that Proposer's Accounting System software has the following interoperability with the current Cook County Jail Management Information System ("CCOMS"):</p> <ul style="list-style-type: none"> - Ability to transmit data to the Proposers system via SFTP, FTPS - Transfer of data must be encrypted - BOIT can allow for direct connection via VPN - Must connect to a 2016 or newer SQL Server database - Must adhere to security standards from Sheriff ISO - Must be able to accept data at 15 minutes intervals to account for housing and custody status changes - Must be able to accept custody status changes in their ordering system to deactivate orders based on status changes. - Minimum Data elements <ol style="list-style-type: none"> 1. Booking Id 2. Inmate ID 3. Inmate Name 4. Bed assignment 5. Meal plan Category 6. Meal Plan Description 7. Effective Date 8. End Date 9. Approved By 10. Date booked 11. Division Assigned 12. Tier Assigned 13. Date Discharged 		
2.9.2	Verify that Proposer's Accounting System software shall electronically transmit Master Menus within thirty (30) days of the award of this contract and annually thereafter upon the anniversary date of the contract award date.		
2.9.2	Verify that Proposer's Accounting System software shall generate a Monthly Usage Report noting usage of products, meals served, and average cost including monthly and year to date data after all transactions (receivers and pulls) for the month are completed and electronically transmit the Monthly Usage Report Summary by the 10th of each month.		
2.9.2	Verify that Proposer's Accounting System software shall electronically transmit a complete Staff roster of all filled and vacant positions, employee names, addresses, and the date each employee begin work in their current position under this contract, with the Staff Roster updated and submitted electronically each month with the monthly billing reports to the CCSO by the 1st of each month.		
2.9.2	Verify that Proposer's Accounting System software shall electronically transmit Standard Operating Procedures within thirty (30) days of the award of this contract.		

Food Service Management System Requirements and Overview			
<i>Please provide a response code and offeror response for each requirement.</i>			
RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
2.9.2	Verify that Proposer's Accounting System software shall electronically transmit portions of the Food Service Staff Meeting Minutes that concern enforcement of CCSO policies, rules, regulations and terms of this agreement to the CCSO in the monthly report.		
2.9.2	Verify that Proposer's Accounting System software shall electronically transmit a report of completed staff training and issued certificates from Proposer to the CCSO by the 10th day of the quarter (January, March, June and September).		
2.9.2	Verify that Proposer's Accounting System software shall electronically transmit a report of detainee initial job orientation training and food handler certification training completion and issued certificates, if any, from Proposer to the CCSO by the 10th of each month.		
2.9.2	Verify that Proposer's Accounting System software shall electronically transmit daily and weekly cleaning schedules developed by the Proposer listing cleaning of areas and equipment in the CCDOC Central Kitchen, ODRs, storage areas, and dock areas that are required to maintain high levels of sanitation, and listing the specific cleaning assignment, day, and shift during which the work will be completed.		
2.9.2	Verify that Proposer's Accounting System software shall electronically transmit Proposer's budget projection report, which estimates food service requirements, serves as the main planning device for food service provided under this contract, and will act as a statement of known requirements for the purchase of supplies at wholesale and for other favorable prices and conditions, by the 15th day of December for the first fiscal quarter, March for the second fiscal quarter, June for the third fiscal quarter, and September for the fourth fiscal quarter.		

Food Service Management System Requirements and Overview			
<i>Please provide a response code and offeror response for each requirement.</i>			
RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
Quality Assurance & Control Plan			
2.10.1	Provide a Quality Assurance and Control Plan to assure contract requirements are met.		
2.10.1	Acknowledge that the Quality Control Plan shall be maintained throughout the duration of the contract and that any amendments to the plan after the contract is awarded shall be submitted to the CCSO two (2) weeks prior to implementation for review and approval		
2.10.1	Describe the policy and procedure for dealing with errors, missing menu/food items on trays or in meal packages, and damaged food.		
2.10.1	Provide a plan for dealing with detainee complaints concerning Food Service products and services at CCDOC.		
2.10.1	Verify that Proposer shall provide grievance statistics for current facilities under contract for containing the largest detainee populations and shall include the facility contact name and phone number of the individual who can verify the reported statistics.		
2.10.1	Verify that Proposer shall conduct a survey of ODR diners quarterly to assess the acceptability of the menus and make adjustments based upon the survey results with the approval of the CCSO, providing that said adjustments have no impact on the cost per meal.		
2.10.1	Verify that Proposer shall observe all rules and regulations regarding storage, preparation and serving of food in the ODR that they are required to observe in the CCDOC Central Kitchen.		
2.10.1	Detail an inspection system covering all of the services required by the contract, including the methods of identifying and preventing deficiencies in the quality of service performed before the level of performance becomes unacceptable; especially meal service.		
2.10.2	Verify that whenever a menu is updated, upon approval the new menu shall be rotated thereafter on a monthly basis to ensure variety.		
2.10.2	Acknowledge that there is no alteration to the menu but for specific "days" such as national holidays or religious holidays.		
2.10.3	Verify that all services performed, and all materials, supplies and equipment furnished or utilized in the performance of services, and all workmanship in the performance of services, shall be performed in a quality manner.		
2.10.3	Acknowledge that all services performed, and all materials, supplies and equipment furnished or utilized in the performance of services, and all workmanship in the performance of services, shall be subject to inspection and test by the CCSO at any time during the performance of the contract.		
2.10.3	Acknowledge that Proposer shall provide full cooperation with any inspector directed by the CCSO or the County to determine the Proposer's conformity with these specifications and the adequacy of the services agreed to.		
2.10.3	Acknowledge that inspections by the CCSO may include inspection by the state, County or city department of public health or any other agency or party authorized or directed by CCSO to inspect the facility		

Food Service Management System Requirements and Overview			
<i>Please provide a response code and offeror response for each requirement.</i>			
RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
Environmental Sustainability			
2.11.1	Acknowledge that the Proposer's work force shall perform services in such a manner as to conserve electricity, gas, water, and steam.		
2.11.1	Submit an Environmental Sustainability Plan that describes the steps Proposer will take to perform the contract in an environmentally sustainable manner.		
2.11.1	Acknowledge that the Environmental Sustainability Plan shall be maintained throughout the duration of the contract, and any amendments to the plan after the contract is awarded shall be submitted to the CCSO two (2) weeks prior to implementation for review and approval.		
2.11.1	Provide a complete list of environmentally sustainable products that Proposer intends to use or supply during performance of the contract, identifying the product, brand/manufacturer and environmental program or standard met for each product.		
2.11.1	Describe how Proposer intends to conserve electricity, gas, water, and steam, as well as reduce the volume and toxicity of waste materials during performance of the contract.		
2.11.1	Acknowledge that Proposer shall be required to participate and integrate with the various waste diversion and recycling programs operated by the CCSO, including efforts intended to divert and reduce food waste.		
2.11.2	Acknowledge that Proposer shall be responsible for utilizing and recycling fibrous (paper and cardboard), plastic, metal and other materials that are recyclable, including food waste in a manner consistent with federal, state, and County standards.		
2.11.2	Acknowledge that Proposer shall, at Proposer's expense, provide, install, and utilize a paper recycling apparatus, which Proposer shall exclusively use to process food service related commodities in a manner consistent with recycling industry standards.		
2.11.2	Acknowledge that Proposer shall be responsible for maintenance and supplies to operate the paper recycling apparatus.		
2.11.2	Acknowledge that Proposer shall provide recycling bins for pre-sorting recyclables, including but not limited to paper, plastic, and aluminum.		
2.11.2	Acknowledge that Proposer's Food Service Director shall participate in weekly facility inspections with the CCSO designee.		
2.11.2	Acknowledge that Proposer shall be responsible for waste management including the proper removal of trash and garbage from the facilities to receptacles located adjacent to the CCDOC Central Kitchen.		
2.11.2	Acknowledge that Proposer shall provide, at their own expense, for scavenger services for removal of all waste generated by the Proposer in the performance of its duties under this contract from CCDOC premises.		
2.11.2	Acknowledge that Proposer shall be responsible for providing all garbage containers/bins, ensuring bins have lids and lids are kept on containers/bins at all times, removing garbage whenever container/bins are full, and keeping containers/bins clean at all times.		

Food Service Management System Requirements and Overview			
<i>Please provide a response code and offeror response for each requirement.</i>			
RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
Good Food Purchasing Program			
2.12	Acknowledge that Proposer shall comply with the Good Food Purchasing Policy and adopt the Good Food Purchasing Standards.		
2.12.1	Submit a Good Food Purchasing Implementation Plan.		
2.12.1	Acknowledge that the Good Food Purchasing Implementation Plan shall be maintained throughout the duration of the contract and any amendments to the plan after the contract is awarded shall be submitted to the CCSO two (2) weeks prior to implementation for review and approval.		
2.12.1	Detail how Proposer will initially meet or exceed the baseline standard set forth in Appendix VII of the RFP for each Good Food Purchasing Standard value category, or if Proposer cannot initially provide product(s) meeting baseline standard(s), Proposer shall outline a plan to meet the standard(s) by the end of the first year of the contract.		
2.12.1	Provide a sample Food Purchasing Data Report, which includes all data fields specified in Section 2.12.1 of the RFP, for each fruit, vegetable, meat/poultry, dairy, and grain product that it intends to use or supply during performance of the contract		
2.12.1	Acknowledge that Proposer shall submit an annual Food Purchasing Data Report, which includes all data fields specified in Section 2.12.1 of the RFP, for each fruit, vegetable, meat/poultry, dairy, and grain product used or supplied during performance of the contract that year.		
2.12.1	Disclose and provide a detailed description of any local, State, or Federal labor and/or environmental violations for which the Proposer has been cited in the last five (5) years.		
2.12.1	Acknowledge that Proposer shall work with the CCSO, the Cook County Department of Public Health, and supporting partner organizations to review and annually update its Good Food Purchasing Implementation Plan in order to continuously work toward a higher score under Good Food Purchasing Standards and Scoring System.		
Non-Compliance			
2.13	<p>Acknowledge that Proposer shall be charged for any or all of the following costs in the event that provided meals and/or meal service are affected by Vendor's late or non-performance of an obligation under Section 2 of this RFP:</p> <ul style="list-style-type: none"> - Any and all actual costs associated with non-compliance, including but not limited to, equipment maintenance or repair costs associated with late or non-performance of an obligation under Section 2.7 (Facilities and Equipment) and mitigation costs associated with late or non-performance of an obligation under Section 2.8 (Sanitation and Pest Control); and - The actual cost of those meals affected on the first day of the late or non-performance of any obligation under Section 2 of this RFP; and - An additional penalty of 10% of the cost of meals affected on the second day of the late or non-performance of any obligation under Section 2 of this RFP. 		

Food Service Management System Requirements and Overview

Please provide a response code and offeror response for each requirement.

RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
Future State Requirements			
4	Solution will interface with the current CCOMS jail management Solution via vendor-recommended method appropriate solution		
4	Solution must provide method where multiple MS SQL databases can consume data from solution via vendor-recommended method appropriate to solution.		
4	Solution must provide an interface to allow CCSO to develop multiple re-useable reports.		
4	Interface must provide the ability to automate running and delivery of these re-useable reports.		
4	Interface must also provide a method allowing CCSO users to construct and run reports on an Ad-hoc basis.		
4	Provide a method to convert Ad-hoc reports into re-useable automated reports.		
4	Solution must possess the capability to read user information from Microsoft's Azure AD.		
4	Solution must possess the capability to update user information – including, but not limited to, user access to system based on user's Azure AD account status		
4	Solution must update itself to grant or deny access based on user's Azure AD account status.		
4	Solution must possess the capability to email notifications, information, and reports to identified individuals via smtp.		

Food Service Management System Requirements and Overview

Please provide a response code and offeror response for each requirement.

RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
Future State Requirements			
Proposed Solution - Solution Overview			
5.1	Proposer presents high level overview of system architecture diagrams for solution not located on CCSO Premises. It is understood that the equipment providing Point of Sale [POS] functionality will be located on CCSO premises. The POS systems must be included in the system architecture diagrams.		
5.1	Proposer presents high level overview of for cloud-based solutions proposer must provide: 1) preferred cloud provider; 2) proposed cloud architecture; 3) security architecture required to protect all data held and transferred to/from proposed solution.		
5.1	Proposer presents high level overview of any required frameworks or other software solution environment support required by proposed solution.		
5.1	Proposer presents high level overview of minimum requirements for front-end and back-end modules.		
5.1	Proposer presents high level overview of interfaces and integration points.		
5.1	Proposer presents high level overview of third party hardware and software included in the proposal or necessary for the proposal.		
5.1	Proposer presents high level overview of other key elements that will help the County better understand the proposed solution.		
Proposed Solution - Software Overview			
5.2	Proposer provides a detailed description of the product(s) and product versions being proposed.		
5.2	Proposer provides details to the system features and capabilities and indicate if these are native to the software or if integration with a 3rd party software is required or recommended.		

Food Service Management System Requirements and Overview

Please provide a response code and offeror response for each requirement.

RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
Proposed Solution - Hosting and Platform Architecture Overview			
5.3	Proposer provides overview of hosting and platform architecture including all environments (production, development, and test) included in the proposal and any differences or limitations in the various environments.		
5.3	Proposer provides overview of hosting and platform architecture including all shared components of the System (e.g., network segments, back-up tapes, etc.).		
5.3	If proposal is cloud-based or hybrid cloud-local solution, the proposer must provide proposed service model (e.g., SaaS, PaaS, IaaS)		
5.3	If proposal is cloud-based or hybrid cloud-local solution, the proposer must provide proposed patching and maintenance service model		
5.3	If proposal is cloud-based or hybrid cloud-local solution, the proposer must provide proposed cloud deployment model		
5.3	If proposal is cloud-based or hybrid cloud-local solution, the proposer must provide any third parties relied upon in the proposed solution (e.g., hosting provider)		
5.3	If proposal is cloud-based or hybrid cloud-local solution, the proposer must provide proposer's rationale for its choice of cloud deployment model		
5.3	If proposal is cloud-based or hybrid cloud-local solution, the proposer must provide how the cloud model might impact the County's data security and BOIT CJIS compliance and associated costs		
Proposed Solution - Integration/Interface			
5.4	Proposers should state cost efficient and financially feasible integration points between the proposed system and the stated existing technologies.		
5.4	Proposers should state the proposed phase/timeline for interface(s) to go live.		
5.4	Proposers must clearly show all integration related costs, alternate integration costs models, and feasible and realistic integration recommendations.		
5.4	Proposers must provide information about any implementation where the proposed solution is interfacing with existing technologies.		

Food Service Management System Requirements and Overview

Please provide a response code and offeror response for each requirement.

RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
Solution Requirements - Hardware and Equipment Requirements			
6.1	If hardware or equipment is included in, or required by, the proposal, then the proposer must describe required hardware and equipment, including minimum specifications of each.		
6.1	If hardware or equipment is included in, or required by, the proposal, then the proposer must describe responsibility for purchasing all hardware and equipment (e.g., proposer or County).		
6.1	If hardware or equipment is included in, or required by, the proposal, then the proposer must describe responsibility for installation of all hardware and equipment (e.g., proposer or County).		
6.1	If hardware or equipment is included in, or required by, the proposal, then the proposer must describe ownership of all hardware and equipment.		
6.1	If hardware or equipment is included in, or required by, the proposal, then the proposer must describe procedures for acceptance, partial shipments and back ordered hardware and equipment.		
6.1	If hardware or equipment is included in, or required by, the proposal, then the proposer must describe warranties and any terms and conditions associated with the hardware and equipment.		
Solution Requirements - Physical Environment Requirements			
6.2	The proposer must describe all physical environment requirements of physical location requirements (e.g., cooling, space, connectivity, etc.)		
6.2	The proposer must describe all physical environment requirements of cabling/wiring and whether the County or Proposer would be responsible for procuring		
6.2	The proposer must describe all physical environment requirements of county's additional power requirements for operating required hardware and equipment		

Food Service Management System Requirements and Overview

Please provide a response code and offeror response for each requirement.

RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
Solution Requirements - Network Requirements			
6.3	The proposer shall include a reasonable estimate of minimum bandwidth required for concurrent application access and data access for “normal” daily operational use for cloud, hybrid and/or on-premise systems.		
6.3	Proposer shall provide its definition of “normal daily operational use.”		
6.3	The proposer shall include a reasonable estimate of peak volume/times for retrieval and uploading transactions.		
6.3	The proposer shall include a reasonable estimate of the typical impact expected on the network post implementation		
6.3	The proposer should describe the optimal physical network infrastructure required to effectively mitigate latency and data speed issues. Describe the vendor provided physical network infrastructure, connectivity testing and performance assurance.		

Food Service Management System Requirements and Overview

Please provide a response code and offeror response for each requirement.

RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
Solution Ownership and Other Terms and Conditions - Data Ownership			
8.1	The selected Proposer will be provided a license access to County Data hereunder for the sole and exclusive purpose of performing its obligations under the resulting Agreement, including a limited non-exclusive, non-transferable license right to transmit, process, and display County Data only to the extent necessary in the provisioning of the Services and not for the storage or recording of County Data.		
8.1	The selected Proposer will be prohibited from disclosing County Data to any third party without specific written approval from the County.		
8.1	The Selected Proposer will have no property interest in, and may assert no lien on or right to withhold County Data from Cook County.		
Solution Ownership and Other Terms and Conditions - Intellectual Property Ownership			
8.2	Proposer must address intellectual property ownership individually with respect to commercial off-the-shelf software or software components		
8.2	Proposer must address intellectual property ownership individually with respect to software customizations		
8.2	Proposer must address intellectual property ownership individually with respect to database schemas		
8.2	Proposer must address intellectual property ownership individually with respect to workflows		
8.2	Proposer must address intellectual property ownership individually with respect to project plans		
8.2	Proposer must address intellectual property ownership individually with respect to documentation		
8.2	Proposer must address intellectual property ownership individually with respect to training materials		
8.2	Proposer must address intellectual property ownership individually with respect to other deliverables		

Food Service Management System Requirements and Overview

Please provide a response code and offeror response for each requirement.

RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
Solution Ownership and Other Terms and Conditions - Hardware and Software Licensing			
8.3	The proposal shall include a clear, high-level, non-legalese explanation of its hardware and software licensing.		
8.3	The proposal shall answer, what type of hardware and software license will the County receive? For example, would the County own licenses after the term of the proposed agreement?		
8.3	The proposal shall answer who are the licensors? For example, is the proposer reselling or integrating a third party's hardware or software?		
8.3	The proposal shall answer, are any conditions attached to the hardware or software licenses? For example, would the County's licenses cease if the County chose to end maintenance services?		
8.3	The proposal shall answer, do any licenses propose to limit the manufacturers' liabilities or the County's remedies?		
Solution Ownership and Other Terms and Conditions - Software and Hardware Warranties			
8.4	The proposal shall include a clear, high-level, non-legalese explanation of its hardware and software warranties.		
8.4	The proposal shall answer, what type of hardware and software warranties will the County receive?		
8.4	The proposal shall answer, what would the warranties cover? If defects only, how are defects defined?		
8.4	The proposal shall answer, what would the warranties exclude?		
8.4	The proposal shall answer, what would be the County's remedies under the warranties? Repair and replace or other?		

Food Service Management System Requirements and Overview

Please provide a response code and offeror response for each requirement.

RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
Solution Ownership and Other Terms and Conditions - Other Terms and Conditions			
8.5	If the proposer requires any additional terms, the proposal shall include a clear, high-level, non-legalese explanation of them.		
8.5	The proposal shall answer, does the proposer intend to impose upon the County any additional terms and conditions, such as end user license agreements, acceptable use policies, terms of service, product use agreements, etc.?		
8.5	The proposal shall answer, does the proposer want to reference its terms and conditions via URL or change its terms and conditions at a later date? Or would the proposer include copies of the additional terms and conditions as exhibits to a contract with the County?		
8.5	The proposal shall answer, do any additional terms limit the proposer's liabilities or the County's remedies?		
8.5	The proposal shall answer, does proposer's system of managing revenue recognitions affect its proposal, including, but not limited to pricing, guarantees, warranty provisions, or compliance with laws?		

Food Service Management System Requirements and Overview

Please provide a response code and offeror response for each requirement.

RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
Solution Performance and Availability - Hosting Services			
9.1	The proposal must describe any hosting services it offers including any necessary information not provided in the hosting and architecture overview.		
9.1	The proposal must describe any hosting services it offers including whether the proposer provides hosting services directly or through a subcontractor; if through a subcontractor, include an explanation of how the proposer ensures its subcontractor will meet requirements of a contract with the County.		
9.1	The proposal must describe any hosting services it offers including the proposer shall clearly state all data storage limits associated with the System. Where exceeding such data storage limits would cause the County to incur additional cost, the proposer shall state such costs in its separate pricing proposal.		
9.1	The proposal must describe any hosting services it offers including The proposer shall clearly state all data transfer limits associated with the System. Where exceeding such data transfer limits would cause the County to incur additional cost, the proposer shall state such costs in its separate pricing proposal.		

Food Service Management System Requirements and Overview

Please provide a response code and offeror response for each requirement.

RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
Solution Performance and Availability - Support and Maintenance Service			
9.2	The proposal must individually address each the following requirements and provide sufficient detail on whether and how it meets the following requirement the proposal must provide multiple tiers of support and must state whether the County is assumed to provide tier 1 support.		
9.2	The proposal must individually address each the following requirements and provide sufficient detail on whether and how it meets the following requirement the proposal must provide support and maintenance response proportionate to varying levels of incident severity.		
9.2	The proposal must individually address each the following requirements and provide sufficient detail on whether and how it meets the following requirement the proposal should provide for multiple methods of reporting an incident to the proposer.		
9.2	The proposal must individually address each the following requirements and provide sufficient detail on whether and how it meets the following requirement if the proposer assumes that the County will provide Tier 1 support, and then the proposer shall deliver sufficient scripts and training to County help desk staff to adequately function as Tier 1 support.		
9.2	The proposal must individually address the following service level agreements (SLAs) for support and maintenance services, including whether such SLAs are offered and any additional cost for the SLAs, and detail on the time it takes an End-User to connect with Respondent's contact center live representative. Respondent will provide toll-free telephone lines in adequate quantity to handle call volume; ACD system(s) to record call date, time and duration information; and electronic interfaces to all systems for monitoring and reporting.		
9.2	The proposal must individually address the following service level agreements (SLAs) for support and maintenance services, including whether such SLAs are offered and any additional cost for the SLAs, and detail on resolution is the time elapsed from the initiation of the Help Desk Incident until Service is restored.		
9.2	The proposal must individually address the following service level agreements (SLAs) for support and maintenance services, including whether such SLAs are offered and any additional cost for the SLAs, and detail on if Proposers offer additional SLAs, they should be included.		
9.2	For each SLA the proposer must detail on how proposer will enable the County to verify SLA compliance.		

Food Service Management System Requirements and Overview

Please provide a response code and offeror response for each requirement.

RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
9.2	For each SLA the proposer must detail any tiering of SLAs, whether by severity or other classification.		
9.2	For each SLA the proposer must whether Proposer offers specific and calculable service level credits, but Proposer must state any credits in its separate pricing proposal.		

Food Service Management System Requirements and Overview

Please provide a response code and offeror response for each requirement.

RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
Solution Performance and Availability - Data Access and Retention			
9.3	The response must state whether Proposer will meet the following data-related system requirement at all times, the County shall be able to receive County data, associated metadata, and reasonably granular subsets thereof, as well as any associated files or attachments, from the System in a useable, encrypted format.		
9.3	The response must state whether Proposer will meet the following data-related system requirement upon termination of the contract and at the County's written request, the Proposer shall destroy County Data, including backups and copies thereof, according to NIST standards or as otherwise directed by the County.		
9.3	The response must state whether Proposer will meet the following data-related system requirement the System shall have the ability to retain County data in a manner that is searchable and capable of compliance with records retention laws and best practices.		
9.3	The response must state whether Proposer will meet the following data-related system requirement at no time may Proposer suspend or terminate County's access to County Data or the System for breach of contract or term or condition relating to the System without giving the County reasonable notice and opportunity to cure according to the County's dispute resolution process.		

Food Service Management System Requirements and Overview

Please provide a response code and offeror response for each requirement.

RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
Solution Performance and Availability - Business Continuity and Disaster Recovery			
9.4	The proposal must individually address each the following requirements and provide sufficient detail on whether and how it meets the following requirement: proposers must have an automated backup and recovery capability for the system and application, including incremental and full backup capabilities. Additionally, system backups must be accomplished without taking the application out of service and without degradation of performance or disruption to County operations.		
9.4	The proposal must individually address each the following requirements and provide sufficient detail on whether and how it meets the following requirement: proposers must be able to provide the service from at least two geographically diverse data centers that do not share common threats (e.g. the data centers cannot be in the same earthquake zone, likely hurricane path, same flood zone, etc.). The data centers must at a minimum meet Tier III standards for redundancy of power, telecommunications, HVAC, security, fire suppression and building integrity.		
9.4	The proposal must individually address each the following requirements and provide sufficient detail on whether and how it meets the following requirement proposers must specify whether, in the event of a technology or other failure at the primary processing center, the alternate system will meet the following tier, for which the County's use should be identical regardless of which location is processing the County's work: High Availability - Continuous operation without interruption or degradation in service.		
9.4	The proposal must individually address each the following requirements and provide sufficient detail on whether and how it meets the following requirement proposers must specify whether, in the event of a technology or other failure at the primary processing center, the alternate system will meet the following tier, for which the County's use should be identical regardless of which location is processing the County's work: Standard Availability - Available for County use within 48 hours with no degradation in service.		
9.4	The proposal must individually address each the following requirements and provide sufficient detail on whether and how it meets the following requirement proposers must specify whether, in the event of a technology or other failure at the primary processing center, the alternate system will meet the following tier, for which the County's use should be identical regardless of which location is processing the County's work: Non-Critical Availability - Available for County use within 96 hours with no degradation in service.		

Food Service Management System Requirements and Overview

Please provide a response code and offeror response for each requirement.

RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
9.4	The proposal must individually address each the following requirements and provide sufficient detail on whether and how it meets the following requirement: proposers must implement crisis management, business continuity and disaster recovery plans, subject to County approval, which the County will not reasonably withhold. These plans must outline how the proposer will support the County's recovery at the alternate site, including backup staff required to implement the plan in an emergency if the proposer's primary staff is unavailable. Such plans shall also include a minimum of annual testing in coordination with the County		
9.4	The proposal must individually address each the following requirements and provide sufficient detail on whether and how it meets the following requirement: proposers must specify the System's proven RTO and RPO in case the primary site becomes unavailable.		
9.4	Proposers must specify whether the System will meet the following availability tiers, which tier, and must specifically describe how the System meets such tier: Category - High Availability, Availability - 99.982%, RTO - intra-day, RPO - typically involves data replication to a hot-site for each transaction or at short intervals, like 15 minutes.		
9.4	Proposers must specify whether the System will meet the following availability tiers, which tier, and must specifically describe how the System meets such tier: Category - Standard Availability, Availability - 99.741%, RTO - 24 to 48 hours, RPO - Nightly tape backups shipped to a warm-site data center. System reestablished at time of disaster from tape. May lose up to one day of data.		
9.4	Proposers must specify whether the System will meet the following availability tiers, which tier, and must specifically describe how the System meets such tier; Category - Non-Critical Availability, Availability - 99.671%, RTO - 48 to 96 hours, RPO - Nightly tape backups shipped to offsite warm or cold site data center. System reestablished at time of disaster from tape after more critical systems are restored. May lose up to one day of data.		

Food Service Management System Requirements and Overview

Please provide a response code and offeror response for each requirement.

RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
Solution Performance and Availability - Transition Out and Exit Requirements			
9.5	The proposal must describe its plan for transitioning Deliverables, County data, and any County intellectual property to the County at the termination of the proposed solution or services, including how the aforementioned would be delivered to the County		
9.5	The proposal must describe its plan for transitioning Deliverables, County data, and any County intellectual property to the County at the termination of the proposed solution or services, including for hosted solutions, the procedure to import County Data to internal site, and the County's responsibilities in the event the County would want to transition to on premise hardware		
9.5	The proposal must describe its plan for transitioning Deliverables, County data, and any County intellectual property to the County at the termination of the proposed solution or services, including whether the Proposer would assist in transition to the County or successor vendor		
9.5	The proposal must describe its plan for transitioning Deliverables, County data, and any County intellectual property to the County at the termination of the proposed solution or services, including how County data in contractors possession would be destroyed after transition		
9.5	The proposal must describe its plan for transitioning Deliverables, County data, and any County intellectual property to the County at the termination of the proposed solution or services, including all assumptions and requirements, such as required time for transition or County participation		
Solution Performance and Availability - Transition of Commencement of Contract			
9.6	The Proposer shall coordinate and cooperate with the County CCSO and the existing Proposer to assure a smooth and orderly transition with uninterrupted food services.		
9.6	Immediately upon award of the contract, the Proposer shall name a Transition Manager who shall have responsibility for transition activities.		
9.6	Within ten (10) days of award of the contract, the Proposer shall submit a Transition Plan to the Executive Director for approval.		

Food Service Management System Requirements and Overview

Please provide a response code and offeror response for each requirement.

RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
Solution Performance and Availability - Continuity of Service			
9.7	Continuity of Service is critical to the CCSO. The successful Proposer must recognize this fact and upon expiration of contract agree to furnish phase-in training to a new Proposer.		
9.7	Continuity of Service is critical to the CCSO. The successful Proposer must recognize this fact and upon expiration of contract agree to exercise best efforts and cooperation for an orderly and efficient transition to a new Proposer.		
9.7	Continuity of Service is critical to the CCSO. The successful Proposer must recognize this fact and upon expiration of contract agree to negotiate in good faith a plan with the successor to determine the nature and extent of the phase-in, phase-out services required.		
9.7	The current Proposer shall provide sufficient experienced personnel during the phase-in, phase out period to ensure that the services called for in the contract are maintained at the required level of proficiency.		
9.7	The current Proposer shall be presumed to be the owner of all supplies, small wares, and food inventories used for the Contract. Proposer shall be free to negotiate with the successor Proposer as to any terms and conditions for sale or transfer of ownership.		

Food Service Management System Requirements and Overview

Please provide a response code and offeror response for each requirement.

RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
Security and Compliance - CCDOC Security Terms and Conditions			
10.1	Proposer agrees to abide by any and all CCSO rules, regulations, policies, and procedures.		
10.1	Proposer shall promptly notify the designated CCSO staff of any security problems or any supervision issues that may have a potential impact upon security		
Security and Compliance - Criminal Background Check			
10.2	All Proposer's employees, sub-vendors, agents and representatives must obtain the appropriate credentials from the CCSO and submit to a background check before commencing work at the CCDOC		
10.2	Proposer shall provide all requested identifying information about new and/or existing employees, sub-vendors, agents and representatives as may be required by the CCSO as a condition of acceptance for a specific employee		
Security and Compliance - Delivery to CCDOC			
10.4	Proposal shall provide that all foodstuffs, goods and other materials deliverable to the County shall be shipped to the CCDOC Central Kitchen, and enter the Cook County Department of Corrections through , Post 8, 3029 South Sacramento Avenue, Chicago, Illinois, 60608		
10.4	Proposer shall pre-notify CCSO Security Staff of all deliveries in accordance with CCSO rules, regulations, policies, and procedures		
10.4	Proposer shall only use plastic pallets at the CCDOC		
10.4	Proposer shall be responsible to for ensuring that foodstuffs, goods, and materials be delivered in clean, intact containers		
10.4	Proposer shall be solely responsible for ensuring that all items it is to provide under the Contract, e.g., foodstuffs, goods, and other materials, that are delivered to the CCSO are of the correct quantities, weights, quality and temperature at point of receipt		

Food Service Management System Requirements and Overview

Please provide a response code and offeror response for each requirement.

RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
Security and Compliance - Data Security Controls			
10.5	Proposal must give an overview of the System's software, hardware, and other controls supporting the System's data security (NIST and CJIS Compliance Standards)		
10.5	Proposer must also provide a reasonably detailed explanation as to how the proposal protects the System and County Data within each of the following additional data security category: Password configurations (e.g., complexity, aging, etc.)		
10.5	Proposer must also provide a reasonably detailed explanation as to how the proposal protects the System and County Data within each of the following additional data security category: Authentication configuration (e.g., active directory, encrypted data exchange, hash, etc.)		
10.5	Proposer must also provide a reasonably detailed explanation as to how the proposal protects the System and County Data within each of the following additional data security category: Encryption configurations (e.g., symmetrical AES-256, asymmetrical RSA 2048, etc.) for both data at rest and data in motion		
10.5	Proposer must also provide a reasonably detailed explanation as to how the proposal protects the System and County Data within each of the following additional data security category: Logging/Auditing capabilities (e.g., verbose user tracking and reporting, etc.)		
10.5	Proposer must also provide a reasonably detailed explanation as to how the proposal protects the System and County Data within each of the following additional data security category: Logs must be exportable to third party log aggregators		
10.5	Proposer must also provide a reasonably detailed explanation as to how the proposal protects the System and County Data within each of the following additional data security category: Physical security (e.g., 24-hour security, alarms, restricted access, etc.)		

Food Service Management System Requirements and Overview

Please provide a response code and offeror response for each requirement.

RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
10.5	Proposer must also provide a reasonably detailed explanation as to how the proposal protects the System and County Data within each of the following additional data security category: Personnel security (e.g., extensive background checks, annual recheck, etc.)		
10.5	Proposer must also provide a reasonably detailed explanation as to how the proposal protects the System and County Data within each of the following additional data security category: Web Application configurations (e.g., SQL injection protection, buffer overflow, etc.)		
10.5	Proposer must also provide a reasonably detailed explanation as to how the proposal protects the System and County Data within each of the following additional data security category: Network transmission security (LAN and VPN)		
10.5	Proposer must also provide a reasonably detailed explanation as to how the proposal protects the System and County Data within each of the following additional data security category: Data that is to be transmitted off-site must be encrypted end to end		
Security and Compliance - Secure Development and Configuration Practices			
10.6	Proposer must describe its application development and configuration practices and how they will reasonably protects the security, confidentiality and privacy of County data and any individuals who may be considered data subjects as to the solution		
10.6	Proposer should state whether it will adhere to the following guidelines: Microsoft Secure Coding Guidelines for the .NET Framework, CERT Secure Coding Standards, OWASP Secure Coding Principles, privacy by design principles, and the Federal Trade Commission's Fair Information Practice Principles		

Food Service Management System Requirements and Overview

Please provide a response code and offeror response for each requirement.

RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
Security and Compliance - Compliance Requirements			
10.7	Proposer must provide sufficient detail on whether and how the proposal possesses data security controls that comply with (If proposer determines any of the following requirements to be inapplicable, proposer shall state so and shall also state the basis for determining each such requirement to be inapplicable): HIPAA, HITECH and the rules promulgated thereunder		
10.7	Proposer must provide sufficient detail on whether and how the proposal possesses data security controls that comply with (If proposer determines any of the following requirements to be inapplicable, proposer shall state so and shall also state the basis for determining each such requirement to be inapplicable): Payment Card Industry standards, including but not limited to PCI DSS and PCI PA-DSS		
10.7	Proposer must provide sufficient detail on whether and how the proposal possesses data security controls that comply with (If proposer determines any of the following requirements to be inapplicable, proposer shall state so and shall also state the basis for determining each such requirement to be inapplicable): 28 CFR 20 and the FBI's CJIS Security Policy		
10.7	Proposer must provide sufficient detail on whether and how the proposal possesses data security controls that comply with (If proposer determines any of the following requirements to be inapplicable, proposer shall state so and shall also state the basis for determining each such requirement to be inapplicable): IRS Publication 1075		
10.7	Proposer must provide sufficient detail on whether and how the proposal possesses data security controls that comply with (If proposer determines any of the following requirements to be inapplicable, proposer shall state so and shall also state the basis for determining each such requirement to be inapplicable): NIST 800-53, as revised		
10.7	Proposer must provide sufficient detail on whether and how the proposal possesses data security controls that comply with (If proposer determines any of the following requirements to be inapplicable, proposer shall state so and shall also state the basis for determining each such requirement to be inapplicable): ISO 27001/27002, as revised		

Food Service Management System Requirements and Overview

Please provide a response code and offeror response for each requirement.

RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
Security and Compliance - Incident Response Requirements			
10.8	Proposer may include a full Incident Response Policy and/or related Plan as an attachment		
10.8	Proposal must state the Proposer's approach to meeting the following data security incident response requirement: Maintenance of the Proposers' Incident Response Plan		
10.8	Proposal must state the Proposer's approach to meeting the following data security incident response requirement: Conformance of such plan to Illinois Personal Information Protection Act and the breach notification laws of the fifty states		
10.8	Proposal must state the Proposer's approach to meeting the following data security incident response requirement: Cook County's rights of review, approval and reasonable modification to Proposer's incident response plan.		
10.8	Proposal must state the Proposer's approach to meeting the following data security incident response requirement: Proposer's approach to provide detailed reports on the nature of incidents and identified data lost or stolen.		
10.8	<p>Proposal must state the Proposer's approach to meeting the following data security incident response requirement: Proposer must describe its plan to address security incidents and data breaches in alignment with the following requirements. For events within the control of Proposer, the Proposer is expected to:</p> <ol style="list-style-type: none"> 1. Immediately notify the County of incidents and breaches. 2. Identify immediate plan of action to mitigate further incident progression. 3. Identify protection measures for affected individuals. 4. Provide outbound and inbound incident-related communications, as requested and directed by the County. 		

Food Service Management System Requirements and Overview

Please provide a response code and offeror response for each requirement.

RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
Security and Compliance - Audit Requirements			
10.9	Proposal must individually address each the following requirements and provide sufficient detail on whether and how it meets the following requirement: The proposer will provide SOC 2, Type 2 reports to the County annually or upon request		
10.9	Proposal must individually address each the following requirements and provide sufficient detail on whether and how it meets the following requirement: The proposer will provide corrective action plans or actions taken to resolve any exceptions, material weaknesses and/or control deficiencies identified in the SOC report		
10.9	Proposal must individually address each the following requirements and provide sufficient detail on whether and how it meets the following requirement: The County will have the right to access and audit proposer's system and hosting		
10.9	Proposal must individually address each the following requirements and provide sufficient detail on whether and how it meets the following requirement: The County will have the right to request reasonable adjustments at the proposer's expense where those requests are based upon audit findings pertaining to the System or Hosting.		

Food Service Management System Requirements and Overview

Please provide a response code and offeror response for each requirement.

RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
Implementation, Development and Project Management Services			
7	Proposer must comply with the County's content management procedures for tracking progress and documents for the duration of the project via either the County's SharePoint site or as otherwise agreed.		
7	Proposer will submit written weekly or monthly status reports to the County, which may include: work accomplished, updated Gantt charts, production goals, accepted deliverables, meetings and minutes, status of risks, issues or problems, summaries of approved project changes, and invoicing and payment.		
Implementation, Development and Project Management Services - Overview of the Implementation Methodology			
7.1	Proposers should depict its implementation strategy in a high level diagram/table and include brief description of proposed methodology		
7.1	Proposers should depict its implementation strategy in a high level diagram/table and include proposed project phases		
7.1	Proposers should depict its implementation strategy in a high level diagram/table and include team roles, including subcontractors		
7.1	Proposers should depict its implementation strategy in a high level diagram/table and include milestones		
7.1	Proposers should depict its implementation strategy in a high level diagram/table and include critical success factors		
7.1	Proposers should depict its implementation strategy in a high level diagram/table and include assumptions		
Implementation, Development and Project Management Services - Project Task List and Timeline			
7.2	Proposers to provide detailed scope tasks/activities, organized in phases including, but not limited to, project management activities, key resources, and estimated hours per key activity.		

Food Service Management System Requirements and Overview

Please provide a response code and offeror response for each requirement.

RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
Implementation, Development and Project Management Services - Assessment, Change Management and Reengineering Approach			
7.3	Proposers should provide a detailed description of your team's approach to assessing and reengineering the County's current state, while concurrently executing a feasible and effective change management plan to include assessment approach		
7.3	Proposers should provide a detailed description of your team's approach to assessing and reengineering the County's current state, while concurrently executing a feasible and effective change management plan to include human change management approach		
7.3	Proposers should provide a detailed description of your team's approach to assessing and reengineering the County's current state, while concurrently executing a feasible and effective change management plan to include reengineering approach		
7.3	Proposers should provide a detailed description of your team's approach to assessing and reengineering the County's current state, while concurrently executing a feasible and effective change management plan to include county responsibilities for the assessment approach, human change management approach, and reengineering approach.		
7.3	Proposers should provide a detailed description of your team's approach to assessing and reengineering the County's current state, while concurrently executing a feasible and effective change management plan to include expected deliverables.		
Implementation, Development and Project Management Services - Requirements Validation and System Design/Configuration			
7.4	Proposers to provide a detailed description of its approach to validating business and technical requirements, including business requirements validation approach and related steps		
7.4	Proposers to provide a detailed description of its approach to validating business and technical requirements, including technical requirements validation approach and related steps		
7.4	Proposers to provide a detailed description of its approach to validating business and technical requirements, including system design approach and related steps		
7.4	Proposers to provide a detailed description of its approach to validating business and technical requirements, including any other key activities		
7.4	Proposer to provide detailed expected Deliverables, the Proposer's and County's respective responsibilities, and acceptance criteria		

Food Service Management System Requirements and Overview

Please provide a response code and offeror response for each requirement.

RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
Implementation, Development and Project Management Services - System Implementation and Configuration			
7.5	Proposers to describe its build and release approach including required level of effort based on the expected configuration and customization work		
7.5	Proposers to describe its build and release approach including software configuration approach including check-in and check-out procedures		
7.5	Proposers to describe its build and release approach including software development approach including check-in and check-out procedures		
7.5	Proposers to describe its build and release approach including system configuration and development management (documentation) procedures		
7.5	Proposers to describe its build and release approach including any other key activity		
7.5	Proposer to provide detailed expected Deliverables, the Proposer's and County's respective responsibilities, and acceptance criteria		
Implementation, Development and Project Management Services - Data Conversion and Migration			
7.6	Proposers to describe the plan for migrating/converting data from existing systems.		
7.6	What County resources do you anticipate will be required for data migration and conversion?		
7.6	What are the County's responsibilities?		
7.6	What is your approach regarding definition of data mapping rules?		
7.6	How does your approach address extraction, transformation, staging, cleansing and validation?		
7.6	Is the County or vendor responsible for cleansing County data prior to migration?		
7.6	What strategies do you employ to conduct the final conversion process?		
7.6	Proposers to describe data migration tasks must be reflected on the project plan and timeline.		
Implementation, Development and Project Management Services - Quality Assurance ("QA")			
7.7	Proposers to provide a detailed description of the proposed QA methodology adhering to best practices and clearly identifying control tasks and testing required to transition functionally from one environment to the next (e.g. dev to prod).		
7.7	Proposers to describe high level proposed QA approach		
7.7	Proposers to describe proposed testing and promotion process		
7.7	Proposers to describe proposed user acceptance process		
7.7	Proposers to describe other key activities		
7.7	Proposer to provide detailed expected Deliverables, the Proposer's and County's respective responsibilities, and acceptance criteria		

Food Service Management System Requirements and Overview

Please provide a response code and offeror response for each requirement.

RFP Req #	Requirement Description	Response Code	Offeror Response Comment(s)
Implementation, Development and Project Management Services - Knowledge Transfer/Training and Transition (Cutover)			
7.8	Proposers to describe the recommended knowledge transfer and change management methodology ensuring County staff participation from the onset of the project.		
7.8	Describe the County's responsibilities and related escalation procedures if/when County participation is not promptly identified.		
7.8	The plan proposers propose should include knowledge transfer approach		
7.8	The plan proposers propose should include end user training approach (including training location, format, total training hours, number of employees trained, timing and signoff process)		
7.8	The plan proposers propose should include administrator training approach (including training location, format, total training hours, number of employees trained, timing and signoff process)		
7.8	The plan proposers propose should include transition/cutover approach		
7.8	The plan proposers propose should include rollout support approach (the County expects on-site support during rollout)		
7.8	Proposer to provide detailed expected Deliverables, the Proposer's and County's respective responsibilities, and acceptance criteria		
Implementation, Development and Project Management Services - Contract Performance Review and Acceptance			
7.9	Proposers should describe all expected contract performance metrics, an approach to collect and transfer all assets to the County, the required key staff to attend close out session(s), and expected close out activities.		
7.9	Proposers close out plan should include list of all expected final documentation and respective acceptance criteria/process		
7.9	Proposers close out plan should include vendor performance review expectations		
7.9	Proposers close out plan should include final project lessons learned review expectations		
7.9	Proposers close out plan should include sample schedule of performance credits for failing to meet SLA and project milestones		