

<p>Subject: RES #663 – Agreement for Use of Live-Scan to Western Identification Network Automated Biometric Identification System with Washington State Patrol</p>	<p>Dept. Origin: Police Department</p> <p>Prepared by: Jennifer Robertson, City Attorney</p> <p>For Agenda of: November 7, 2017</p> <p>Exhibits: RES #663, Agreement & Attached Document</p>
<p>Proposed Council Action:</p> <p>Adopt Resolution #663.</p>	<p style="text-align: right;">Initial & Date</p> <p>Concurred by Mayor: _____</p> <p>Approved by City Planner: _____</p> <p>Approved as to form by City Atty: <u>JSR/11-1-17</u></p> <p>Approved by Finance Director: _____</p> <p>Approved by Department Head: _____</p>

INFORMATION / BACKGROUND

Under the Interlocal Cooperation Act,¹ the City may contract with other jurisdictions to do anything that the City is permitted to do. The Ruston Police Department has been provided the opportunity to obtain live-scan fingerprinting equipment from the Washington State Patrol (WSP) and to utilize the Western Identification Network (WIN) for Automated Biometric Identification System (ABIS) services as part of the User Agreement.

Under the Agreement, WSP will furnish (on long term loan) to the City a live-scan fingerprinting machine and related equipment to capture fingerprint images and related information of a person arrested, registering as a sex or kidnapping offender, applying for licensing or employment pursuant to state or local requirements (“Applicant Submissions”), or as required for the emergency placement of children pursuant to law. WSP will also allow the City to utilize its network connection and upload images to fingerprint databases maintained by law enforcement and to obtain information from the same for law enforcement purposes. WSP will provide training to the City for using the system.

The Agreement is valid until June 30, 2022 unless otherwise terminated by WSP or by mutual agreement of the parties. At termination, the City will return the equipment to WSP. The City is required pay for the costs of installation and to ensure that the system is secure. The City is also required to follow WSP security protocols for ensuring the security of the system.

Under the Agreement, the City is required to indemnify WSP and the State of Washington for any claims, etc. that arise out of any misuse of the databases, errors in fingerprint identification

¹ Chapter 39.34 RCW.

made by the City, “or any cause of action whatsoever, and against any loss, cost, expense, and damage resulting therefrom, including attorney’s fees.” (Hold Harmless Section, p. 3.)

The lack of reciprocal termination and indemnification provisions in the Agreement are less than ideal from the City Attorney’s perspective, thus the City requested these provides be made reciprocal. The WSP has declined to amend the Agreement. The Chief believes this will be an important law enforcement tool and will save the City money, so recommends the Agreement be approved.

Also in your packet are the User Access Acknowledgment, CJIS Security Policy and the WIN-33 Input and Output Implementation Guide. These are attached to the Agreement.

FISCAL CONSIDERATION

The City would need to pay for yearly maintenance at a cost around \$1,200 and an initial installation cost of \$2,250. These are costs the City would incur if it bought its own machine. The installation cost can be shared by the police and court budgets. The police budget would be utilized for annual maintenance costs.

BOARD OR COMMITTEE RECOMMENDATION

None.

RECOMMENDATION / MOTION

Approve Resolution #663.

MOTION: I move to approve Resolution #663 authorizing the Mayor to execute a contract with the Washington State Patrol for use of the live-scan to Western Identification Network Automated Biometric Identification System.

RESOLUTION NO. 663

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF RUSTON, WASHINGTON, AUTHORIZING THE MAYOR TO EXECUTE AN AGREEMENT WITH THE WASHINGTON STATE PATROL FOR USE OF WESTERN IDENTIFICATION NETWORK AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (WIN ABIS).

WHEREAS, in accordance with Chapter 39.34 RCW, the “Interlocal Cooperation Act”, the City is authorized to contract with other governmental agencies to provide services that the City is authorized to perform; and

WHEREAS, the Ruston Police Department has been provided the opportunity to obtain live-scan fingerprinting equipment and to utilize the Western Identification Network (WIN) for Automated Biometric Identification System (ABIS) services through a services agreement with the Washington State Patrol (WSP); and

WHEREAS, the Ruston Police Chief recommends entering into this Agreement as it will likely save the City money and will also result in the City gaining a useable and valuable asset by obtaining this device from WSP; and

WHEREAS, the City Council finds it in the public interest to authorize the Mayor to execute the proposed Agreement with WSP for use of WIN ABIS which is attached to this Resolution as Exhibit “1”;

NOW, THEREFORE, THE CITY COUNCIL OF THE CITY OF RUSTON, WASHINGTON, DOES HEREBY RESOLVE AS FOLLOWS:

Section 1. Authorization of Agreement. The Mayor is hereby authorized to execute the Agreement with the Washington State Patrol for WIN ABIS Services in substantially the form attached hereto as Exhibit "1".

Section 2. Posting on Website Required. The Clerk is directed to post a copy of this Agreement, once fully executed, on the City's website.

RESOLVED this 7th day of November, 2017.

APPROVED:

Bruce Hopkins, Mayor

ATTEST/AUTHENTICATED:

Judy Grams, City Clerk

FILED WITH THE CITY CLERK: 11/01/2017
PASSED BY THE CITY COUNCIL: _____
RESOLUTION NO.: 663

Attachment “1”

2017 Revised Agreement for Special Police Services

Between

City of Ruston and Pierce County Sheriff’s Office

**WASHINGTON STATE PATROL
LIVE-SCAN TO WESTERN IDENTIFICATION NETWORK AUTOMATED BIOMETRIC
IDENTIFICATION SYSTEM (WIN ABIS) CONNECTION USER'S AGREEMENT**

THIS AGREEMENT, entered into between the Washington State Patrol (hereinafter referred to as "WSP"), an agency of the State of Washington; and the Ruston Police Department, (hereinafter referred to as "the User"), witnesses that:

1. WSP is an agency of the State of Washington authorized by law to establish and operate an Automated Biometric Identification System (hereinafter referred to as "ABIS") capable of, but not limited to, reading, classifying, matching, and storing fingerprints, and to maintain criminal history record information based on fingerprint identification. ABIS is a state-funded system comprised of a central computer processor located at the WSP in Olympia. The criminal history repository is known as the Washington State Identification System (WASIS) and maintained by WSP in Olympia.
2. WSP has entered into agreement with the Western Identification Network (WIN) for ABIS services. The WIN ABIS is a multi-state funded system comprised of a host system presently located in Rancho Cordova, California (the WIN Central Site) with remote input stations and booking terminals in member states as authorized by the WIN Board of Directors.
3. The User operates live-scan fingerprinting equipment to capture fingerprint images and related information of a person arrested, registering as a sex or kidnapping offender, applying for licensing or employment pursuant to state or local requirements ("Applicant Submissions"), or as required for the emergency placement of children pursuant to the Adam Walsh Child Protection and Safety Act of 2006, Section 151.

NOW THEREFORE, in light of the foregoing representations and the promises, conditions, and other valuable considerations more fully set out or incorporated herein by reference, the parties, by their duly authorized officials, do mutually agree as follows:

1. WSP will furnish the User, a criminal justice agency as defined in chapter 10.97 RCW, with such criminal justice information as is available in WASIS, ABIS and WIN ABIS files. WSP will serve as the means of exchange of computerized criminal history information and fingerprint data.
2. The network connection will be made via an e-mail server administered by WSP. This network and local networks will meet the requirements of Criminal Justice Information Services (CJIS) Security Policy. The User shall notify WSP of sustained or repeated network problems that affect this service.
3. The User will submit the fingerprint images and the related information electronically to the WSP for the purpose of identification and, when applicable, inclusion in the ABIS, WASIS and WIN ABIS databases. For Applicant Submissions requiring a fee, the User agrees to establish a fingerprint services billing account with WSP. By establishing a billing account for fingerprint image submissions, the User agrees to collect, hold, and reconcile fees charged by WSP for the type of applicant fingerprints submitted by the User. If a transmission is sent in error, the User is still responsible for all fees associated with the transaction type.

4. The User agrees that WSP will provide authorization for access to the ABIS, WASIS and WIN ABIS databases with certain restrictions depending on system capabilities and assigned status as follows:
 - A. Local live-scan sites will submit fingerprint images and related information for identification search and inclusion in the ABIS, WASIS and WIN ABIS databases.
 - B. The User agrees to comply with statutory mandates concerning the submission of criminal and civil fingerprint submissions to WSP.
5. The User agrees that only the WSP site or authorized remote sites may permanently register fingerprints into the ABIS, WASIS and WIN ABIS databases.
6. The WSP ABIS Coordinator or designee will provide the User with policies including, but not limited to, a schedule for accessing the ABIS, WASIS and WIN ABIS databases. Such policies shall define the basis and procedures for conducting routine and emergency comparison of fingerprints against these databases.
7. The User shall take necessary measures to make its live-scan equipment and system secure and prevent unauthorized use. WSP reserves the right to object to equipment security measures and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP.
8. Livescan equipment is the property of WSP and is on loan to the user. The User agrees to pay installation costs and purchase maintenance from the live-scan vendor for the loaned live-scan equipment for as long as the user utilizes the device.
9. The User agrees to assign a live-scan coordinator to serve as the primary contact person for the User in Live-Scan to ABIS connection-related issues. The User also agrees to notify WSP immediately, in writing, of any changes in this position.
10. WSP agrees to schedule and provide training of equipment and procedures to User personnel at locations and times arranged by WSP. Equipment operation training may be supplied by WSP or the equipment provider.
11. The User shall access and utilize ABIS, WASIS and WIN ABIS databases only in conjunction with the administration of criminal justice as authorized by laws governing criminal history dissemination.
12. Fingerprint identification or criminal history information records provided to the User under this Agreement shall not be further disseminated by the User to any other person or (private or public) entity, except as required in criminal proceedings or pursuant to state or federal law.

PERIOD OF PERFORMANCE

This Agreement becomes effective on the date of the last signature and continues until June 30, 2022 or until termination as provided herein.

COMPLIANCE WITH LAWS, REGULATIONS AND PROCEDURES

The User agrees to comply with all applicable federal and state laws, regulations, rules, and procedures, and to assume certain costs associated with the User's use of the services described herein. The User shall operate livescan equipment and otherwise conduct itself in strict compliance with applicable policies and procedures published by WIN and WSP including: the Policies and Procedures of WIN ABIS as currently in force; the Washington State Patrol (WSP) Access User Acknowledgment, and the policies and procedures identified in this Agreement.

The Policies and Procedures of WIN ABIS are hereby incorporated into and made a part of this Agreement except to the extent that they are inconsistent with anything found herein. The User will comply with related FBI Criminal Justice Information Services Security (CJIS) Policy and other security practices adopted by WIN as these relate to ABIS, WASIS and WIN ABIS.

SUSPENSION AND TERMINATION

WSP may suspend further performance of services hereunder when, in its reasonable estimation, the User has breached any material term of the Agreement. For the purposes of this Agreement, the violation of any specific term of this Agreement or of any substantive requirement or limitation imposed by the federal or state statutes, regulations, or rules incorporated into this Agreement shall be deemed a breach of a material term of the Agreement.

WSP may terminate this Agreement if the User commits any material breach of any term of this Agreement, which breach is not cured within thirty (30) business days after receipt of notice from WSP. Both parties may, by mutual agreement, terminate this Agreement on terms then acceptable to them.

Upon termination of this Agreement for any reason, each party shall promptly return to the other any property that belongs to the other party. With respect to hardware or software products that are the property of WSP or WIN, the User shall promptly return such property to WSP.

Neither WIN, WSP nor the User shall be liable for (i) any indirect, incidental, consequential or special damages under this agreement arising solely from the termination of this Agreement in accordance with its terms.

HOLD HARMLESS

The User agrees to hold harmless the Western Identification Network and its employees; and the State of Washington, the Washington State Patrol and its employees from and against any and all claims, demands, actions, suits, including but not limited to, any liability for damages by reason of or arising out of any misuse of the ABIS, WASIS and WIN ABIS databases, erroneous fingerprint identifications made by user personnel, or any cause of action whatsoever, and against any loss, cost, expense, and damage resulting therefrom, including attorney's fees.

This agreement replaces any previous agreement between WSP and the User on this subject.

IN WITNESS THEREOF, the duly authorized officials of the respective parties have executed this written Agreement.

RUSTON POLICE DEPARTMENT

WASHINGTON STATE PATROL

BY _____

TITLE _____

Simon Tee, Grants and Contracts Manager

DATE _____

APPROVED AS TO FORM BY THE OFFICE OF THE ATTORNEY GENERAL 6/2/2010



WASHINGTON STATE PATROL ACCESS USER ACKNOWLEDGMENT

I. Introduction

Since its inception, the National Crime Information Center (NCIC) has operated under a shared management concept between the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division and state users. The NCIC Advisory Policy Board established a single state agency in each state to assume responsibility as the NCIC CJIS Systems Agency (CSA) for all agencies within the state. The CSA is responsible for the planning of necessary hardware, software, funding, security, auditing, and training of all authorized agencies within the state for complete access to FBI CJIS systems data services. The Washington State Patrol (WSP) Criminal Records Division (CRD) Administrator is designated as the NCIC CJIS Systems Officer (CSO). The FBI CJIS Division requires the CSO to manage the following:

1. Operational, technical, and investigative assistance to NCIC users
2. Telecommunications lines to a state interface
3. Legal and legislative review of matters pertaining to NCIC
4. Timely distribution of information related to all aspects of NCIC system usage by means of the ACCESS Operations Manual, NCIC Operating Manual, CJIS Security Policy, Technical and Operational Updates, and related documents
5. Training and training materials to all participating agencies
6. System security to include physical security, personnel, and all technical aspects of security as required in the CJIS Security Policy

The following documents are incorporated by reference and made part of this user acknowledgment:

1. ACCESS Operations Manual
2. CJIS Security Policy
3. U.S. Code of Federal Regulations, Title 28, Part 20
4. Applicable federal and state laws and regulations; ACCESS/WACIC rules, regulations, and policies as recommended by the ACCESS Section

II. Primary Connection and Originating Agency Identifier (ORI) Issuance

All agencies that inquire on or enter data into ACCESS must have a primary connection to ACCESS and a signed WSP ACCESS User Acknowledgment on file prior to adding secondary connections such as regional management systems. Agencies must ensure that all system use through both the primary or secondary connections remain in compliance with ACCESS and FBI CJIS rules.

The CSO will coordinate the assignment of new ORI numbers, the change in ORI location or address, and any other changes, cancellations, or retirements of ORIs accessing WACIC/NCIC. The assignment of an ORI to an agency is not a guarantee of access to the state and federal systems. The CSA makes the final determination of who may access WACIC/NCIC based on the standards provided by the CJIS Security Policy and determination of an agency's administration of criminal justice. Any requests for additional ORIs by an agency will be forwarded to the WSP ACCESS Section Manager, who will

conduct a short audit of the agency to verify compliance standards are being met. See ACCESS Operations Manual Introduction for more information.

III. Indemnification

Each agency(party) shall defend, protect, and hold harmless the other agency(party) from and against all claims, suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this agreement.

IV. Administrative Responsibilities

The agency shall respond to requests for information by the FBI CJIS Division or ACCESS in the form of questionnaires, surveys, or similar methods, to the maximum extent possible, consistent with any fiscal, time, or personnel constraints of that agency.

All agencies are required to have formalized written procedures for the following, if applicable: validations, hit confirmation, criminal history use and dissemination, ACCESS misuse, record entry (for all record types entered into WACIC and NCIC), rebackground investigations, password management, disposal of media, physical protection and documenting, updating the system network.

The CSO provides system training to agencies accessing WACIC/NCIC through the state computer system. If employees are using inquiry only functions, they must attend Level 1 certification training. Employees entering information into the WACIC/NCIC system must attend Level 2 certification training. All certifications must be acquired within six months of hire date and renewed biennially. All staff who manage ACCESS users and are not ACCESS certified must view the Upper Management and Administrators Overview Training online and sign the signature log, which must be kept at the agency for review during the triennial ACCESS audit.

Security awareness training is required within six months of initial assignment, and biennially thereafter, for all personnel (who are not ACCESS certified) that have unescorted access to CJI. This includes agency employees, custodial staff, IT staff, upper management, etc. Records of individual basic security awareness training shall be documented, kept current, and maintained by each agency for review during the triennial ACCESS or Technical Security audit.

A Terminal Agency Coordinator (TAC) must be assigned for each terminal agency. This person is the Point Of Contact (POC) for the agency. A TAC must maintain a Level 2 ACCESS certification. The TAC retains the responsibility of ensuring his/her agency is in compliance with state and FBI CJIS Division policies and regulations. A TAC must attend TAC training once during the triennial audit cycle.

For those agencies providing ACCESS services through regional computer systems to outside agencies, the TAC shall be responsible for the dissemination of all administrative messages received on the 24 hour printer to those agencies.

The CSO provides the criminal justice community with the current ACCESS Operations Manual, NCIC Operating Manual, NCIC Code Manual, and CJIS Security Policy. Manual updates are provided on a quarterly basis. The agency shall incorporate such changes upon receipt. Information is provided via email and can be found on the ACCESS website at the following link:

V. Criminal History Record Information (CHRI) Responsibilities

Each agency shall conform to system policies, as established by the FBI CJIS Division and ACCESS, before access to CHRI is permitted. This will allow for control over the data and give assurance of system security.

1. The rules and procedures governing terminal access to CHRI shall apply equally to all participants in the system.
2. All criminal justice agencies with ACCESS terminals and access to computerized CHRI data from the system shall permit an FBI CJIS Division and an ACCESS audit team to conduct appropriate audits. Agencies must cooperate with these audits and respond promptly.
3. All terminals interfaced directly with the ACCESS/WACIC/NCIC systems for the exchange of CHRI must be under the management control of a criminal justice agency, as defined by the CJIS Security Policy.
4. All agencies must ensure they provide all required information when running criminal history checks. WSP retains access to all agency criminal history logs through the ACCESS System. Secondary dissemination of criminal history must be logged by the agency.

VI. Record Entry Responsibilities

Record Quality

Criminal justice agencies have a specific duty to maintain records that are accurate, complete, and current. ACCESS recommends agencies conduct self audits as a means of verifying the completeness and accuracy of the information in the system. These self assessments should be on a continual basis to ensure both quality assurance and compliance with standards. Errors discovered in NCIC records are classified as serious errors, form errors, or an error trend.

Serious errors: FBI CJIS will cancel the record and notify the entering agency via administrative message. The message provides the entire canceled record and a detailed explanation of the reason for cancellation.

Form errors or error trends: The CSA notifies the ORI by letter of the corrective action to be taken. No further notification or action will be taken by the CSA, unless the CSA deems it appropriate.

Timeliness

WACIC/NCIC records must be entered promptly to ensure maximum system effectiveness. Records must be entered according to standards defined in the ACCESS Operations Manual.

Accuracy and Completeness

The accuracy of WACIC/NCIC data must be double checked and documented, including the initials and date by a second party. The verification should include assuring the data in the WACIC/NCIC record matches the data in the investigative report and that other checks were made. Agencies lacking support staff for second party checks should require the case officer to check the record.

Complete records of any kind include all information available on the person or property at the time of entry. ACCESS recommends “packing the record” for all entries. Complete inquiries on persons include numbers that could be indexed in the record (i.e. Social Security Number (SSN), Vehicle Identification Number (VIN), Drivers License Number (OLN), etc.). Inquiries should be made on all names/aliases used by the suspect. Complete vehicle inquiries include VIN and license plate numbers.

Record Validations

NCIC/WACIC validation listing are prepared pursuant to a schedule, as published in the ACCESS Operations Manual. These listings are distributed to the originating agency via File Transfer Protocol (FTP).

Validation requires the originating agency to confirm the record is complete, accurate, and active. Validation is accomplished by reviewing the original entry and current supporting documents, and correspondence with any appropriate complainant, victim, prosecutor, court, motor vehicle registry files, or other appropriate source or individual. Validation efforts must be well documented. Validation efforts include what was done to complete the validation of the individual record. Documentation of phone calls, letters, dates and dispositions need to be included with each record that was validated. Many agencies document this information in the case file. In the event the agency is unsuccessful in its attempts to contact the victim, complainant, etc., the entering agency must make a determination based on the best information and knowledge available whether or not to retain the original entry in the file.

The agency must sign the validation certificate and fax, mail, or email a copy to the ACCESS Section each month certifying the records were validated. If the CSA has not received a validation certificate response from an agency within the specified period of time, the CSA will purge all records which are the subject of that agency’s validation listings from NCIC and WACIC.

VII. Security Responsibilities

Technical Roles and Responsibilities

All agencies participating in ACCESS must comply with and enforce system security. Each interface agency (city, county, or other agency) having access to a criminal justice network must have someone designated as the technical security POC. A criminal justice network is a telecommunications infrastructure dedicated to the use by criminal justice entities exchanging criminal justice information. The technical security POC’s shall be responsible for the following:

1. Identifying the user of the hardware/software and ensuring that no unauthorized users have access to the same
2. Identifying and documenting how the equipment is connected to the state system
3. Ensuring that personnel security screening procedures are being followed as stated in the CJIS Security Policy
4. Ensuring that appropriate hardware security measures are in place
5. Supporting policy compliance and keeping the WSP Information Security Officer (ISO) informed of security incidents

Security Enforcement

Each interface agency is responsible for enforcing system security standards for their agency, in addition to all of the other agencies and entities to which the interface agency provides CJIS and Washington State Department of Licensing (DOL) records information. Authorized users shall access CJIS and DOL systems and disseminate the data only for the purpose for which they are authorized. Each criminal justice and non-criminal justice agency authorized to access FBI CJIS systems and DOL shall have a written policy for the discipline of policy violators.

Physical Security

A physically secure location is a facility 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.

The perimeter of a physically secure location shall be prominently posted and separated from non-secure locations by physical controls.

All personnel with access to computer centers, terminal areas, and/or areas where CJIS information is housed shall either be escorted by authorized personnel at all times or receive a fingerprint-based background check and view security awareness training.

Personnel Security

To verify identification, a state of residency and national fingerprint-based record checks shall be conducted within 30 days of initial employment or assignment for all personnel who have authorized access to FBI CJIS systems and those who have direct responsibility to configure and maintain computer systems and networks with access to FBI CJIS systems. All requests for system access shall be made as specified by the CSO. The CSO or their official designee is authorized to approve CJIS systems access. All official designees to the CSO shall be from an authorized criminal justice agency.

Support personnel, contractors, and custodial workers who access computer terminal areas shall be subject to a state of residency and national fingerprint-based record check and view the security awareness training, unless these individuals are escorted by authorized personnel at all times. Authorized personnel are those persons who have passed a state and national fingerprint-based record check and have been granted access.

Private Contractors/Vendors

Private contractors shall be permitted access to CJIS record information systems pursuant to an agreement which specifically identifies the contractor's purpose and scope of providing services for the administration of criminal justice. The agreement between the criminal justice government agency and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI. Private contractors who perform the administration of criminal justice 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.

Hit Confirmation

Any agency that enters a record into NCIC/WACIC has the duty to promptly respond with the necessary confirmation of the hit and other details. They must furnish a response within a specific time period. Valid hit confirmation is based on two levels of priority: urgent or routine.

Priority 1: Urgent

The hit must be confirmed within ten minutes. In those instances where the hit is the only basis for detaining a suspect or the nature of a case requires urgent confirmation of a hit, priority 1 should be specified.

Priority 2: Routine

The hit must be confirmed within one hour. Generally, this priority will be used when the person is being held on local charges, property has been located under circumstances where immediate action is not necessary, or an urgent confirmation is not required.

VIII. Compliance Audits

The FBI CJIS Division requires triennial audits be conducted by the CSA to review CJIS standards of compliance and provide recommendations for best business practices. WSP audit staff provide three types of reviews:

1. **Agency Compliance Review:** WSP Auditors conduct an administrative interview with the TAC. The interview includes questions to determine adherence to WACIC/NCIC policy requirements including:
 - a. TAC responsibilities
 - b. ACCESS certification, rebackground of ACCESS users and other trainings
 - c. System security
 - d. Media protection
 - e. Criminal history
 - f. National Instant Criminal background Check System (NICS)
 - g. Random sample of missing persons in WACIC/NCIC
 - h. Random sample of warrants in WACIC/NCIC
 - i. Random sample of protection orders in WACIC/NCIC
 - j. Random sample of stolen vehicles in WACIC/NCIC
 - k. Record maintenance
 - l. Hit confirmation
 - m. ORI usage and administration of criminal justice functions
 - n. Written procedures
 - o. Validations
 - p. Site security visits to ensure terminal locations are secure
2. **Data Quality Review:** WSP Auditors conduct an on-site data quality review. Auditors compare WACIC/NCIC records against agency case files. Auditors check for accuracy, completeness, and verify entry and removal practices. The auditors document records with errors for the agency to update.
3. **Auditor Recommendations for Best Practices:** WSP Auditors provide a compliance report of information received during the interview and data quality review. They provide recommendations for best business practices.

IX. Technical Security Audits

The agency is responsible for compliance to technical standards set forth by ACCESS and the CJIS Security Policy. Technical security audits will follow the WACIC/NCIC triennial audit schedule.

1. **Agency Compliance Review:** The WSP ISO performs security audits addressing the following compliance areas:
 - a. Personnel security measures
 - b. Security incident response
 - c. Configuration management control
 - d. Encryption
 - e. Media protection (physical and electronic)
 - f. Physical protection
 - g. Session lock capabilities
 - h. System and communications protection and information integrity
 - i. Boundary protection
 - j. Malicious code protection
 - k. Event logging capability
 - l. System use notification
 - m. Patch management
 - n. Identification and authentication
 - o. Wireless devices – mobile / bluetooth / cellular
 - p. Partitioning and virtualization
 - q. Cloud computing



WSP ACCESS USER ACKNOWLEDGMENT

As an agency head/director, I hereby acknowledge the duties and responsibilities as set forth in this ACCESS User Acknowledgement, as well as those documents incorporated by reference. I acknowledge that these duties and responsibilities have been developed to ensure the reliability, confidentiality, completeness, and accuracy of all records contained in or obtained by means of the WACIC/NCIC system. I also acknowledge that a failure to comply with these duties and responsibilities will subject my agency to various sanctions. These sanctions may include the termination of ACCESS/WACIC/NCIC services to my agency.

I further understand DOL may review activities of any person who receives vehicle, vessel, and firearm record information to ensure compliance with limitations imposed on the use of the information. The DOL shall suspend or revoke for up to five years the privilege of obtaining information of a person found to be in violation of chapter 42.56 RCW, chapter 46.12 RCW, or the user agreement with DOL. I understand misuse of this information is a gross misdemeanor and is punishable by a fine not to exceed \$10,000 or by imprisonment in a county jail not to exceed one year, or both such fine and imprisonment for each violation. RCW 46.12.640.

Agency Name:		
ORI:		
Agency Head Name (printed):		
Agency Head Email:		
Agency Head Telephone Number:		
Agency Head Signature		Date:

Please return a copy of this signature page to the WSP ACCESS Section.

24x7 Hit Confirmation Agreement

Must be completed by agencies who:

- A. Provide 24/7 teletype printer coverage for another agency.**
- B. Receive 24/7 teletype printer coverage from another agency.**

Every terminal agency that enters records destined for NCIC/WACIC must ensure hit confirmation is available for all records, except III, 24 hours per day either at the agency or through a written agreement with another agency at its location. The terminal agency printer must be monitored 24 hours per day. In the event that 24 hour per day hit confirmation coverage is not available, the terminal agency printer must be capable of being forwarded to a 24 hour a day facility. A 24 hour telephone number of the agency responsible for confirming hits must be placed in the Miscellaneous Field of every entry.

Parties who enter into this agreement must adhere to the response times and regulations set forth in the ACCESS Operations Manual and the CJIS Security Policy. This interagency agreement must be current and approved by the CJIS Systems Agency (CSA), the Washington State Patrol (WSP) before agencies adopt the policies and procedures set forth by the agreement.

Termination of Agreement

This agreement shall remain in effect unless terminated by either agency upon thirty (30) days written notice. The agency terminating the agreement must also formally notify the WSP ACCESS Section within the thirty (30) days. Termination of this agreement requires the agency printer to be forwarded to another 24 hour per day facility.

I hereby acknowledge the responsibility and duty to perform teletype hit confirmation to the terminal agency 24 hours per day within the requirements defined by NCIC/WACIC and the CJIS Security Policy.

Agency Providing 24/7 Coverage:		
ORI:		
Agency Head Name (printed):		
Agency Head Signature:		Date:

Agency Receiving 24/7 Coverage:		
ORI:		
Agency Head Name (printed):		
Agency Head Signature:		Date:

Holder of the Record Agreement

Must be completed by agencies who:

- A. Use their ORI to enter another agency's records.**
- B. Have their records entered under another agency's ORI.**

A Holder of the Record Agreement (HORA) is required when an agency uses their ORI to enter another agency's records, thus becoming the holder of the record. The holder of the record is defined as an agency that is using their ORI to enter another agency's records. The owner of a record is defined as the agency where the record originated.

The purpose of this agreement is to establish responsibility for records entered in WACIC/NCIC by the holder of record under its NCIC assigned ORI on behalf of the owner of record. As they relate to records entered for the owner of record, the holder of record assumes the following responsibilities: data entry; documentation; cancellation and modification of entries; timeliness of entries, cancellations and modifications; hit confirmation; second party checks; and validation of entries. The owner of the record is also responsible for providing the HORA with information for entry in a timely manner.

The holder of record must adhere to the regulations set forth in the ACCESS Operations Manual and the CJIS Security Policy. This interagency agreement must be current and approved by the CJIS Systems Agency (CSA), the Washington State Patrol (WSP) before agencies adopt the policies and procedures set forth by the agreement.

Entries provided under the HORA (check all that apply):

- | | | | |
|---------------------------------------------|-----------------------------------------------|--------------------------------------------|---------------------------------------------|
| <input type="checkbox"/> All entries | <input type="checkbox"/> Articles | <input type="checkbox"/> Boats | <input type="checkbox"/> Gangs |
| <input type="checkbox"/> Guns | <input type="checkbox"/> Identity Theft | <input type="checkbox"/> Images | <input type="checkbox"/> License Plates |
| <input type="checkbox"/> Missing Persons | <input type="checkbox"/> Person of Interest | <input type="checkbox"/> Protection Orders | <input type="checkbox"/> Securities |
| <input type="checkbox"/> Supervised Persons | <input type="checkbox"/> Unidentified Persons | <input type="checkbox"/> Vehicles | <input type="checkbox"/> Vehicle/Boat Parts |
| <input type="checkbox"/> Wanted Persons | <input type="checkbox"/> Violent Persons | | |

Termination of Agreement

This agreement shall remain in effect unless terminated by either agency upon thirty (30) days written notice. The agency terminating the agreement must also formally notify the WSP ACCESS Section within the thirty (30) days. Termination of this Agreement shall not negate the obligation of either party to maintain records entered under this agreement to ensure their accuracy and timeliness.

Agency Acting as the Holder of the Record:			
ORI:			
Agency Head Name (printed):			
Agency Head Signature:			Date:

Agency Acting as the Owner of the Record:			
ORI:			
Agency Head Name (printed):			
Agency Head Signature:			Date:

Inter-agency Agreement

Must be completed by agencies who:

- A. Provide criminal justice services to another agency.**
- B. Receive criminal justice services from another agency.**

An inter-agency agreement describing the criminal justice services provided and/or received by an agency must be in place.

Agency Providing Service: _____

Agency Receiving Service: _____

Services Provided (check all that apply):

- | | |
|-----------------------------------------------------|-------------------------------------------------------------------------|
| <input type="checkbox"/> Hit confirmation | <input type="checkbox"/> Gun transfers/Concealed Pistol Licenses (CPLs) |
| <input type="checkbox"/> Dispatch | <input type="checkbox"/> Use of regional management system |
| <input type="checkbox"/> Record entry | <input type="checkbox"/> Terminal connection to ACCESS |
| <input type="checkbox"/> Record validations | <input type="checkbox"/> Information Technology (IT) services |
| <input type="checkbox"/> Other services (describe): | |

Parties who enter into this agreement must adhere to the regulations set forth in the ACCESS Operations Manual and the CJIS Security Policy. This interagency agreement must be current and approved by the CJIS Systems Agency (CSA), the Washington State Patrol (WSP) before agencies adopt the policies and procedures set forth by the agreement.

Termination of Agreement

This agreement shall remain in effect unless terminated by either agency upon thirty (30) days written notice. The agency terminating the agreement must also formally notify the WSP ACCESS Section within the thirty (30) days.

Agency Providing Criminal Justice Service(s):		
ORI:		
Agency Head Name (printed):		
Agency Head Signature:		Date:

Agency Receiving Criminal Justice Service(s):		
ORI:		
Agency Head Name (printed):		
Agency Head Signature:		Date:

Management Control Agreement

Must be completed by agencies who:

- A. Have a city or county Information Technology (IT) department handling IT services for the criminal justice agency.**

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 A Central Computerized Enforcement Service System (ACCESS) for the interstate exchange of criminal history/criminal justice information, the Criminal Justice Agency shall have the authority, via managed control, to set and enforce:

- (1) Priorities.
- (2) Standards for the selection, supervision, and elimination of access to personnel who may be tasked with working on or interfacing with any of the telecommunication systems or criminal justice systems/computers enumerated in paragraph three below.
- (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.

Responsibility for management of security control shall remain with the criminal justice agency, as required by the CJIS Security Policy.

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.

Agency Providing IT Service(s):		
Agency Head Name (printed):		
Agency Head Signature:		Date:

Criminal Justice Agency Receiving IT Service(s):		
ORI:		
Agency Head Name (printed):		
Agency Head Signature:		Date:

Information Exchange Agreement

Must be completed by agencies who:

A. Provide criminal justice information to contracted prosecutors.

An information exchange agreement describing the Criminal Justice Information (CJI) provided and/or received by an agency must be in place between the agency providing the information and the contracted prosecutor receiving the information.

1. Security Control: Each person receiving the information will maintain the information in a physically secure location and only authorized individuals will have access to the CJI. The information will not be left in the open for unauthorized individuals to view.
2. Misuse: Each person receiving the information will use the information for criminal justice purposes only. The information received is not to be used in any civil cases or disseminated to non criminal justice personnel.
3. Training: Each person receiving the information will be responsible to view the Basic Security Awareness Training once every two years. The training log will be provided by and maintained at the criminal justice agency providing the CJI for review at the audit.
4. Destruction: CJI shall be securely disposed of when no longer required and destroyed by shredding or incineration.

Services Provided (check all that apply):

- Criminal History Other CJI (describe):
-

Parties who enter into this agreement must adhere to the regulations set forth in the ACCESS/NCIC Operating Manuals and the CJIS Security Policy. This Information Exchange Agreement must be current and approved by the CJIS Systems Agency (CSA), the Washington State Patrol (WSP) before agencies adopt the policies and procedures set forth by the agreement.

Termination of Agreement

This agreement shall remain in effect unless terminated by either party upon thirty (30) days written notice.

Agency Providing Criminal Justice Information:		
ORI:		
Agency Head Name (printed):		
Agency Head Signature:		Date:

Contracted Prosecutor Receiving Criminal Justice Information:		
Contractor Name (printed):		
Contractor Signature:		Date:

City Named in the Contract		
Authorizing Name (printed):		
Authorizing Signature:		Date:



Criminal Justice Information Services (CJIS) Security Policy

Version 5.6
06/05/2017

CJISD-ITS-DOC-08140-5.6



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
5.0	Policy Rewrite	Security Policy Working Group	02/09/2011	See Signature Page
5.1	Incorporate Calendar Year 2011 APB approved changes and administrative changes	CJIS ISO Program Office	07/13/2012	APB & Compact Council
5.2	Incorporate Calendar Year 2012 APB approved changes and administrative changes	CJIS ISO Program Office	08/09/2013	APB & Compact Council
5.3	Incorporate Calendar Year 2013 APB approved changes and administrative changes	CJIS ISO Program Office	08/04/2014	APB & Compact Council
5.4	Incorporate Calendar Year 2014 APB approved changes and administrative changes	CJIS ISO Program Office	10/06/2015	APB & Compact Council
5.5	Incorporate Calendar Year 2015 APB approved changes and administrative changes	CJIS ISO Program Office	06/01/2016	APB & Compact Council
5.6	Incorporate Calendar Year 2016 APB approved changes and administrative changes	CJIS ISO Program Office	06/05/2017	APB & Compact Council

SUMMARY OF CHANGES

Version 5.6

APB Approved Changes

1. Section 5.6.2.1 Standard Authenticators: add language concerning tokens and one-time passwords, Fall 2016, APB16, SA4, Standard Authenticator Use in the CJIS Security Policy.
2. Section 5.6.2.1 Standard Authenticators: add new Section 5.6.2.1.3 One-time Passwords (OTP), Fall 2016, APB16, SA4, Standard Authenticator Use in the CJIS Security Policy.
3. Section 5.10.1.2 Encryption: modify language in section, Spring 2016, APB15, SA4, Clarifying Encryption Requirements in the CJIS Security Policy.
4. Section 5.10.1.2.1 Encryption for CJI in Transit: create new section and realign requirements, Spring 2016, APB14, SA4, Clarifying Encryption Requirements in the CJIS Security Policy.
5. Section 5.10.1.2.2 Encryption for CJI at Rest: create new section and realign requirements, Spring 2016, APB15, SA4, Clarifying Encryption Requirements in the CJIS Security Policy.
6. Section 5.10.1.2.2 Encryption for CJI at Rest: remove the reference to National Security Agency (NSA) Suite B Cryptography, Fall 2016, APB16, SA2, Update to Encryption for Criminal Justice Information (CJI) at Rest.
7. Section 5.10.1.2.3 Public Key Infrastructure (PKI) Technology: create new section and add language, Spring 2016, APB15, SA4, Clarifying Encryption Requirements in the CJIS Security Policy.
8. Appendix A Terms and Definitions: add new definitions – “Asymmetric Encryption”, “Hybrid Encryption”, “Symmetric Encryption”, Spring 2016, APB15, SA4, Clarifying Encryption Requirements in the CJIS Security Policy.
9. Appendix B Acronyms: add new acronyms – “OTP – One-time Password”, Fall 2016, APB16, SA4, Standard Authenticator Use in the CJIS Security Policy,
10. Appendix G.3 Cloud Computing: modify language throughout the appendix, Fall 2016, APB16, SA3, Encrypting CJI Stored or Accessed within a Cloud Environment.
11. Appendix G.6 Encryption: create a new best practices appendix, Spring 2016, APB15, SA4, Clarifying Encryption Requirements in the CJIS Security Policy.

Administrative Changes¹

1. Section 5.1.1.4, change “inter-agency” to “interagency” for consistency.
2. Section 5.1.2, change “inter-agency” to “interagency” for consistency.
3. Section 5.10.1.1 Boundary Protection: bullet 5, modify language, “(i.e. the device ~~shall~~ “~~fail~~fails open” vs. “~~fail~~fails closed”).”
4. Section 5.11 Formal Audits: add new Section 5.11.4 Compliance Subcommittees and add language
5. Section 5.11.4 References/Citations/Directives: renumber to Section 5.11.5

¹ Administrative changes are vetted through the Security and Access Subcommittee and not the entire APB process.

6. Section 5.12.1.1 Minimum Screening Requirements for Individuals Requiring Access to CJI: bullet 6, remove language “, and, if applicable, the appropriate board maintaining management control,”
7. Section 5.13.1.1 802.11 Wireless Protocols: change “80.11i” to “802.11i”
8. Appendix A Terms and Definitions: add new definitions – “Decryption”, “Encryption”
9. Appendix G.6 Encryption: Add language describing FIPS-140-2 certification

KEY TO APB APPROVED CHANGES (e.g. “Fall 2013, APB11, SA6, Future CSP for Mobile Devices”):

Fall 2013 – Advisory Policy Board cycle and year

APB## – Advisory Policy Board Topic number

SA# – Security and Access Subcommittee Topic number

Topic Title

TABLE OF CONTENTS

Executive Summary	i
Change Management	ii
Summary of Changes	iii
Table of Contents	v
List of Figures	xi
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
5.1.5	References/Citations/Directives	19
5.2	Policy Area 2: Security Awareness Training.....	20
5.2.1	Awareness Topics	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	20
5.2.1.4	Level Four Security Awareness Training	21
5.2.2	Security Training Records.....	22
5.2.3	References/Citations/Directives	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
5.3.5	References/Citations/Directives	26
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
5.4.8	References/Citations/Directives	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	34
5.5.7	References/Citations/Directives	34
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).....	36
5.6.2.1.3	One-time Passwords (OTP)	37
5.6.2.2	Advanced Authentication.....	37
5.6.2.2.1	Advanced Authentication Policy and Rationale	37
5.6.2.2.2	Advanced Authentication Decision Tree	38
5.6.3	Identifier and Authenticator Management	40
5.6.3.1	Identifier Management.....	40
5.6.3.2	Authenticator Management.....	40
5.6.4	Assertions	40
5.6.5	References/Citations/Directives	41
5.7	Policy Area 7: Configuration Management	47
5.7.1	Access Restrictions for Changes	47
5.7.1.1	Least Functionality.....	47
5.7.1.2	Network Diagram.....	47
5.7.2	Security of Configuration Documentation	47
5.7.3	References/Citations/Directives	47
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
5.8.5	References/Citations/Directives	50
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
5.9.3	References/Citations/Directives	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	56
5.10.1.4	Voice over Internet Protocol.....	56
5.10.1.5	Cloud Computing.....	56
5.10.2	Facsimile Transmission of CJI.....	56
5.10.3	Partitioning and Virtualization	57
5.10.3.1	Partitioning.....	57
5.10.3.2	Virtualization	57
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.....	58
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.....	59
5.10.5	References/Citations/Directives	59
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
5.11.5	References/Citations/Directives	62
5.12	Policy Area 12: Personnel Security	63
5.12.1	Personnel Security Policy and Procedures	63
5.12.1.1	Minimum Screening Requirements for Individuals Requiring Access to CJI:..	63

5.12.1.2 Personnel Screening for Contractors and Vendors	64
5.12.2 Personnel Termination	64
5.12.3 Personnel Transfer.....	65
5.12.4 Personnel Sanctions.....	65
5.12.5 References/Citations/Directives	65
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.....	71
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
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.....	41
Figure 9 – Authentication Decision for Known Location	45
Figure 10 – Authentication Decision for Unknown Location	46
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.....	59
Figure 15 – The Audit of a Local Police Department.....	62
Figure 16 – A Local Police Department's Personnel Security Controls	65

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.

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 publically 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 CJI. 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.

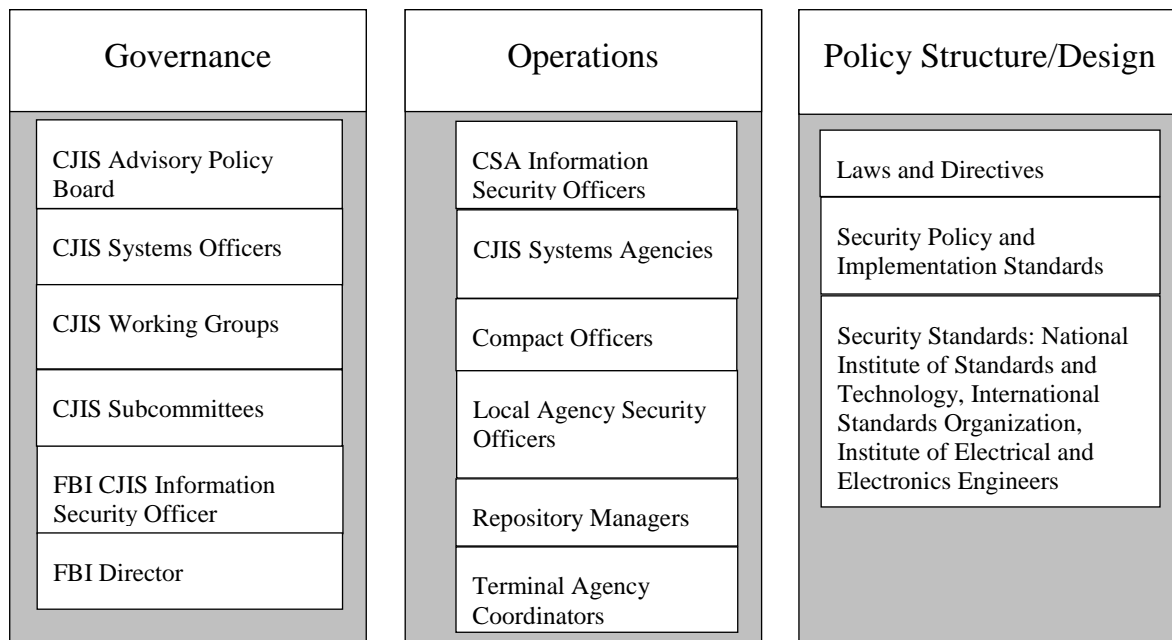


Figure 1 – Overview Diagram of Strategic Functions and Policy Components

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. The CSO, or designee, shall ensure that a Terminal Agency Coordinator (TAC) is designated within each agency that has devices accessing CJIS systems.
 - e. Ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO).
 - f. Approve access to FBI CJIS systems.
 - g. Assume ultimate responsibility for managing the security of CJIS systems within their state and/or agency.
 - h. 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 re-certification 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, FNU, 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.

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 per authorization of Department of Justice (DOJ) Order 0904. 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 per authorization of Department of Justice (DOJ) Order 0904.

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.

5.1.5 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

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

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.

5.2.1 Awareness Topics

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 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.

5.2.3 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

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.

5.3.5 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

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 CJJ.

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.
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.

5.4.8 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

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 CJJ 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 CJIS.

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 5.10.2 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:

- (i) the system use information is available and when appropriate, is displayed before granting access;
- (ii) any references to monitoring, recording, or auditing are in keeping with privacy accommodations for such systems that generally prohibit those activities; and
- (iii) 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.

5.5.7 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

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

Agencies shall follow the secure password attributes, below, to authenticate an individual's unique ID. 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.

5.6.2.1.2 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.

- a. Be a minimum of six (6) digits
- b. Have no repeating digits (i.e., 112233)
- c. Have no sequential patterns (i.e., 123456)
- d. Not be the same as the Userid.
- e. 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.
- f. Not be identical to the previous three (3) PINs.
- g. Not be transmitted in the clear outside the secure location.

- h. 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.

- a. Be a minimum of six (6) randomly generated characters
- b. Be valid for a single session
- c. 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:**

- a. A user, irrespective of his/her location, accesses the LEEP portal. The LEEP has AA built into its services and requires AA prior to granting access. AA is required.
- b. 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.

5.6.5 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

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

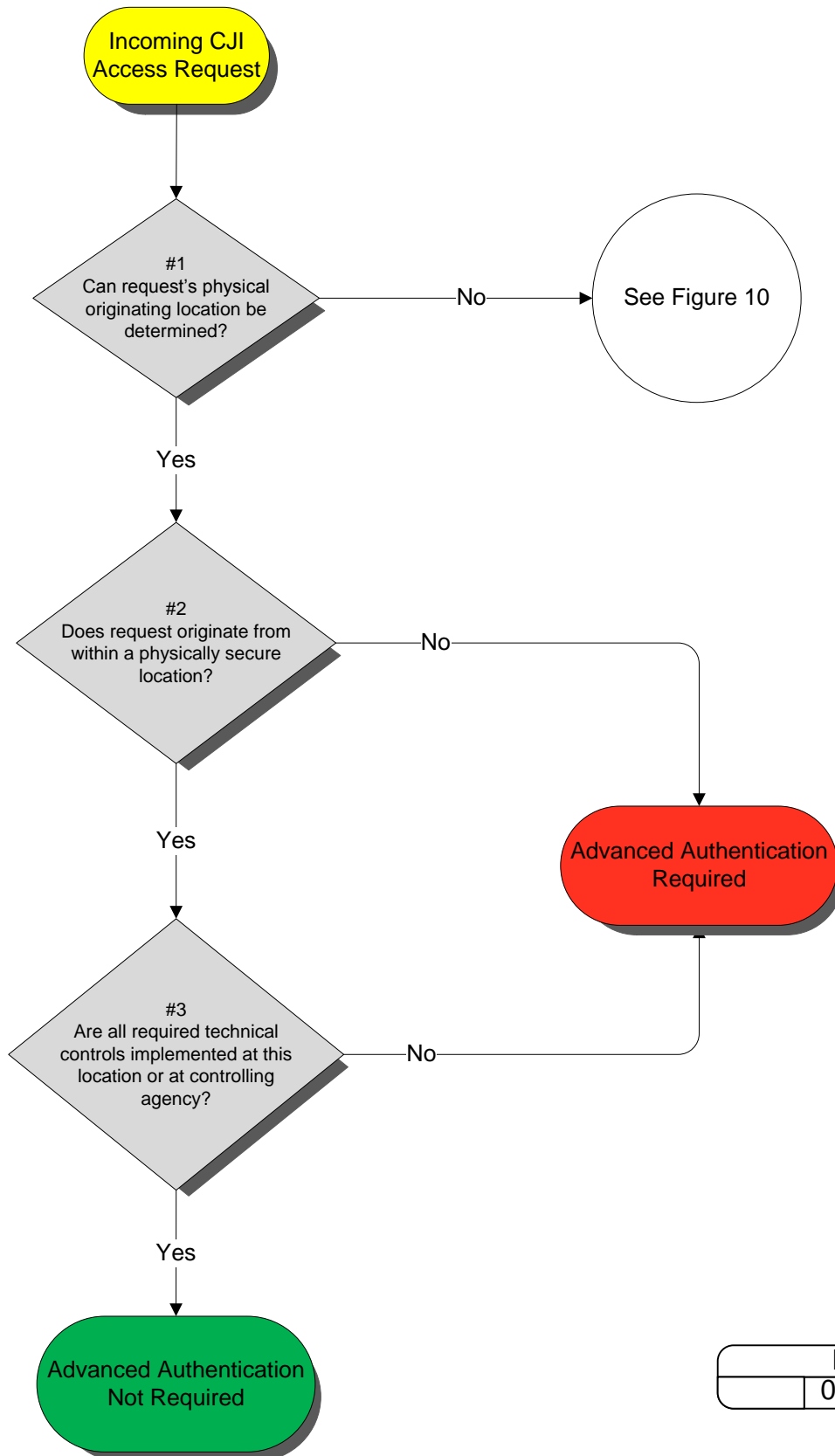


Figure 9		
	08/04/2014	

Figure 10 – Authentication Decision for Unknown Location

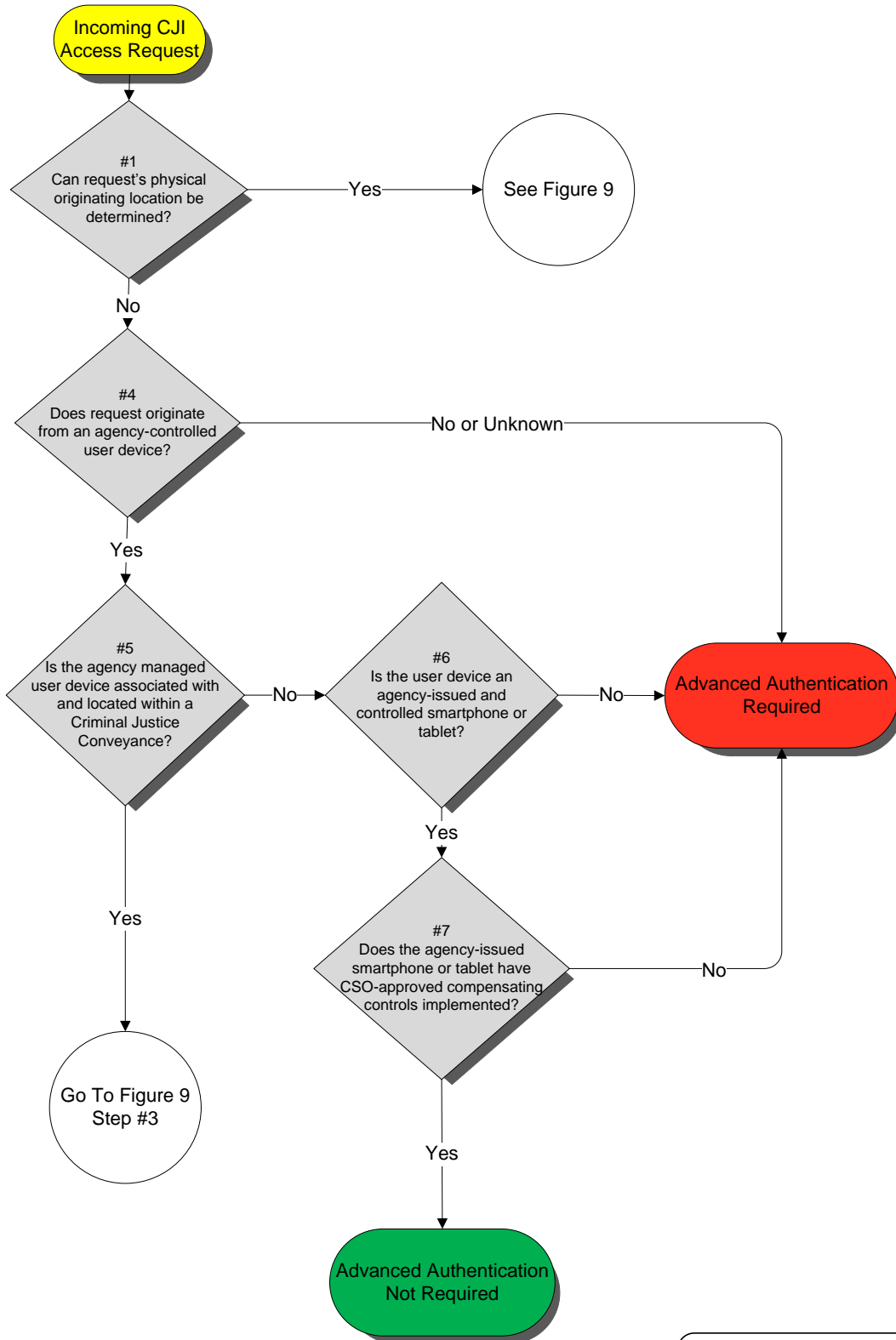


Figure 10		
	10/06/2015	

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.

5.7.3 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

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.

5.8.5 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

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.

5.9.3 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

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:

- a) See Sections 5.13.1.2.2 and 5.10.2.
- b) Encryption shall not be required if the transmission medium meets all of the following requirements:
 - i. The agency owns, operates, manages, or protects the medium.
 - ii. Medium terminates within physically secure locations at both ends with no interconnections between.
 - iii. Physical access to the medium is controlled by the agency using the requirements in Sections 5.9.1 and 5.12.
 - iv. 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.
 - v. 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.

- a) When agencies implement encryption on CJI at rest, the passphrase used to unlock the cipher shall meet the following requirements:
 - i. Be at least 10 characters
 - ii. Not be a dictionary word.
 - iii. Include at least one (1) upper case letter, one (1) lower case letter, one (1) number, and one (1) special character.
 - iv. Be changed when previously authorized personnel no longer require access.
- b) 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:

- a) Include authorization by a supervisor or a responsible official.
- b) Be accomplished by a secure process that verifies the identity of the certificate holder.
- c) Ensure the certificate is issued to the intended party.

5.10.1.3 Intrusion Detection Tools and Techniques

The agency shall implement network-based and/or host-based intrusion detection tools.

The CSA/SIB shall, in addition:

1. Monitor inbound and outbound communications for unusual or unauthorized activities.
2. Send individual intrusion detection logs to a central logging facility where correlation and analysis will be accomplished as a system wide intrusion detection effort.
3. 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 metadata derived from CJI shall not be used by any cloud service provider for any purposes. The cloud service provider shall be prohibited from scanning any email or data files for the purpose of building analytics, data mining, advertising, or improving the services provided.

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 background 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.

5.10.5 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

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 CJJ 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 CJI, 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.

5.11.5 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

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 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 Security Policy and Procedures

5.12.1.1 Minimum Screening Requirements for Individuals Requiring Access to CJI:

1. To verify identification, a state of residency and national fingerprint-based record checks shall be conducted within 30 days of assignment for all personnel who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI. 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:
 - (i) 5 CFR 731.106; and/or
 - (ii) Office of Personnel Management policy, regulations, and guidance; and/or
 - (iii) agency policy, regulations, and guidance.

(See Appendix J for applicable guidance regarding noncriminal justice agencies performing adjudication of civil fingerprint submissions.) Federal entities bypassing state repositories in compliance with federal law may not be required to conduct a state fingerprint-based record check.

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 felony conviction of any kind exists, the hiring authority in the Interface Agency shall deny access to CJI. However, the hiring authority 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.
4. If a record of any other 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.
5. 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.
6. If the person is employed by a NCJA, the CSO or his/her designee shall review the matter to determine if CJI access is appropriate. This same procedure applies if this person is found to be a fugitive or has an arrest history without conviction.
7. 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.

8. 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.
9. Support personnel, contractors, and custodial workers with access to physically secure locations or controlled areas (during CJI processing) shall be subject to a state and national fingerprint-based record check unless these individuals are escorted by authorized personnel at all times.

It is recommended individual background re-investigations be conducted every five years unless Rap Back is implemented.

5.12.1.2 Personnel Screening for Contractors and Vendors

In addition to meeting the requirements in paragraph 5.12.1.1, contractors and vendors shall meet the following requirements:

1. Prior to granting access to CJI, the CGA on whose behalf the Contractor is retained shall verify identification via a state of residency and national fingerprint-based record check. 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.
2. If a record of any kind is found, 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-appointed Security Officer.
3. When identification of the applicant with a criminal history has been established by fingerprint comparison, the CGA or the CJA (if the CGA does not have the authority to view CHRI) shall review the matter.
4. A Contractor employee found to have a criminal record consisting of felony conviction(s) shall be disqualified.
5. Applicants shall also be disqualified on the basis of confirmations that arrest warrants are outstanding for such applicants.
6. The CGA shall maintain a list of personnel who have been authorized access to CJI and shall, upon request, provide a current copy of the access list to the CSO.

Applicants with a record of misdemeanor offense(s) may be granted access if the CSO determines the nature or severity of the misdemeanor offense(s) do not warrant disqualification. The CGA may request the CSO to review a denial of access determination.

5.12.2 Personnel Termination

The agency, upon termination of individual employment, shall immediately terminate access to CJI.

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.

5.12.5 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

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:
 - i. Remote locking of device
 - ii. Remote wiping of device
 - iii. Setting and locking device configuration
 - iv. Detection of “rooted” and “jailbroken” devices
 - v. Enforcement of folder or disk level encryption
 - vi. Application of mandatory policy settings on the device
 - vii. Detection of unauthorized configurations
 - viii. Detection of unauthorized software or applications
 - ix. Ability to determine the location of agency controlled devices
 - x. Prevention of unpatched devices from accessing CJI or CJI systems
 - xi. Automatic device wiping after a specified number of failed access attempts

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 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 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.

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

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 proposed compensating controls for AA are a combination of controls that provide 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.

At least two of the following examples of AA compensating controls for agency-issued smartphones and tablets with limited feature operating systems shall be implemented to qualify for compensating control consideration:

- Possession of the agency issued smartphone or tablet as an indication it is the authorized user
- Implemented password protection on the Mobile Device Management application and/or secure container where the authentication application is stored
- Enable remote device locking
- Enable remote data deletion
- Enable automatic data wipe after predetermined number of failed authentication attempts
- Remote device location (GPS) tracking
- Require CJIS Security Policy compliant password to access the device
- Use of device certificates as per Section 5.13.7.3 Device Certificates

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 CJJ. 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 CJJ. 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 CJJ.

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 CJI, 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 CJI, 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 CJI 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 CJ. 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 CJ. 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, FNU, 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).

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.

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.

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.

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.

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 CJI, this usually refers to one of the applications that can be used to process CJI.

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 CJI, 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.

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.

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.

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

DoJCERT	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
HTTP	Hypertext Transfer Protocol
IAFIS	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
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OMB	Office of Management and Budget
ORI	Originating Agency Identifier
OTP	One-time Password
PBX	Private Branch Exchange
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
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
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 CJJ, 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

Overview: Conceptual Connections Between Various Agencies

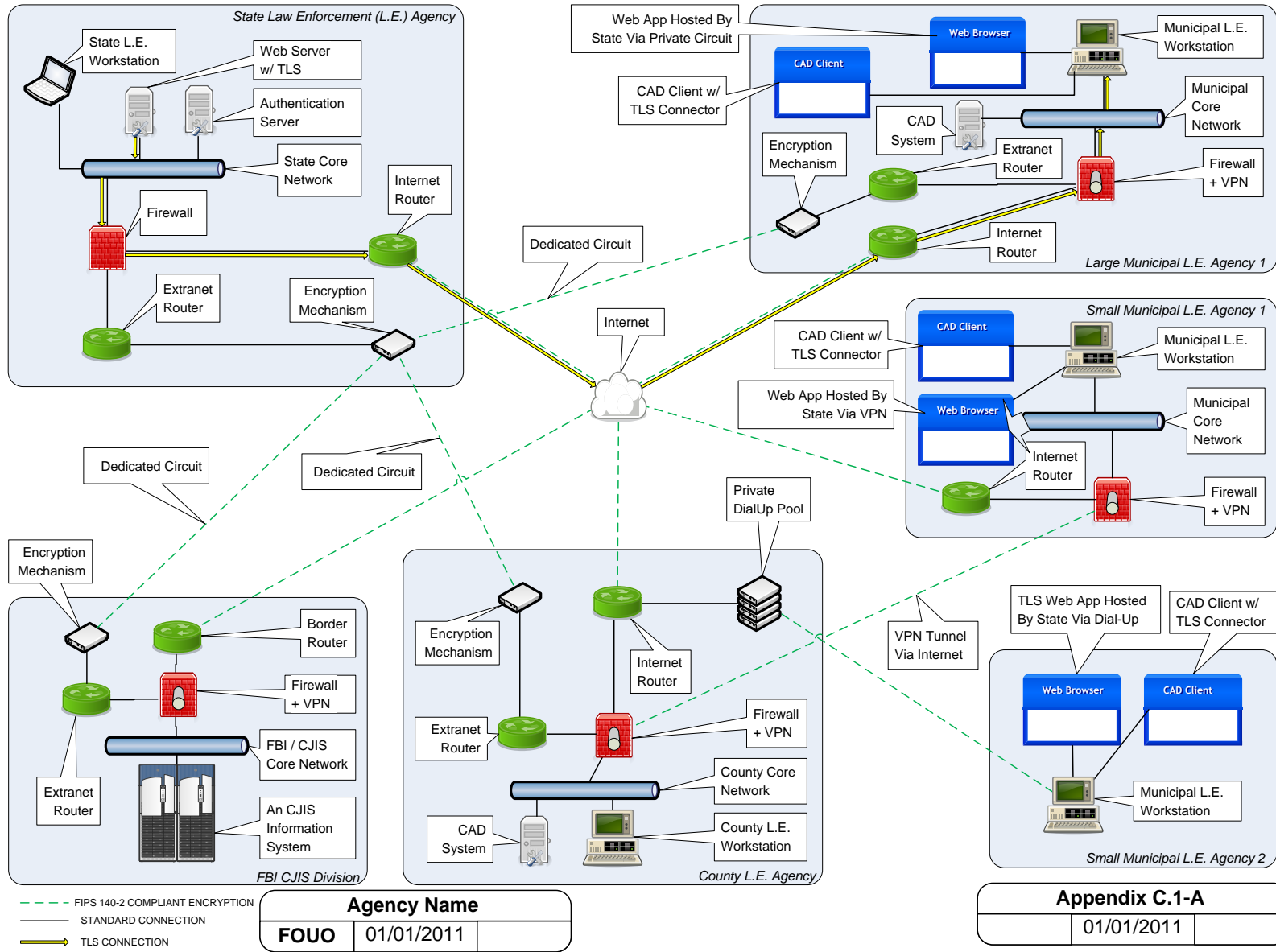
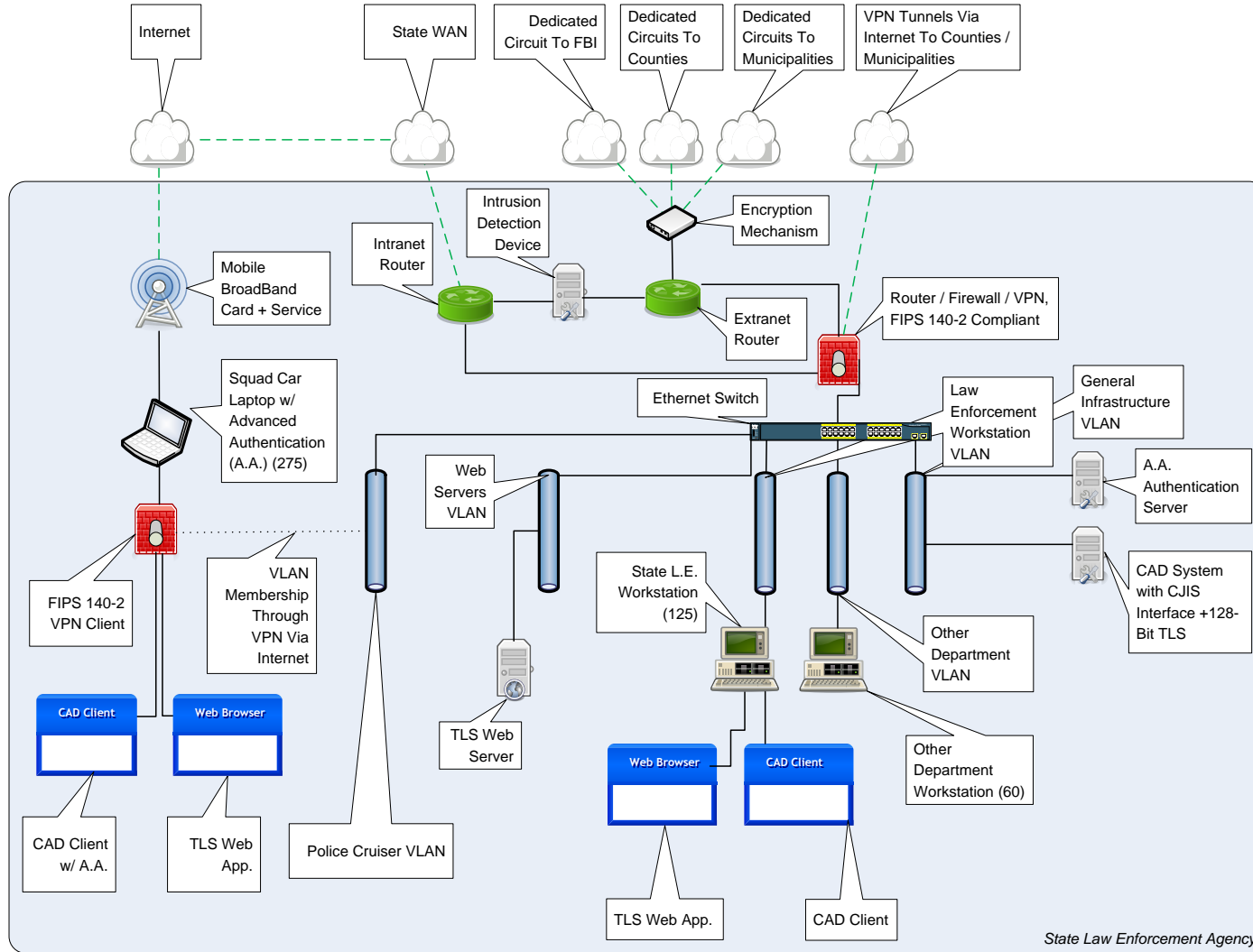


Figure C-1-B Conceptual Topology Diagram for a State Law Enforcement Agency

Conceptual Topology Diagram For A State Law Enforcement Agency



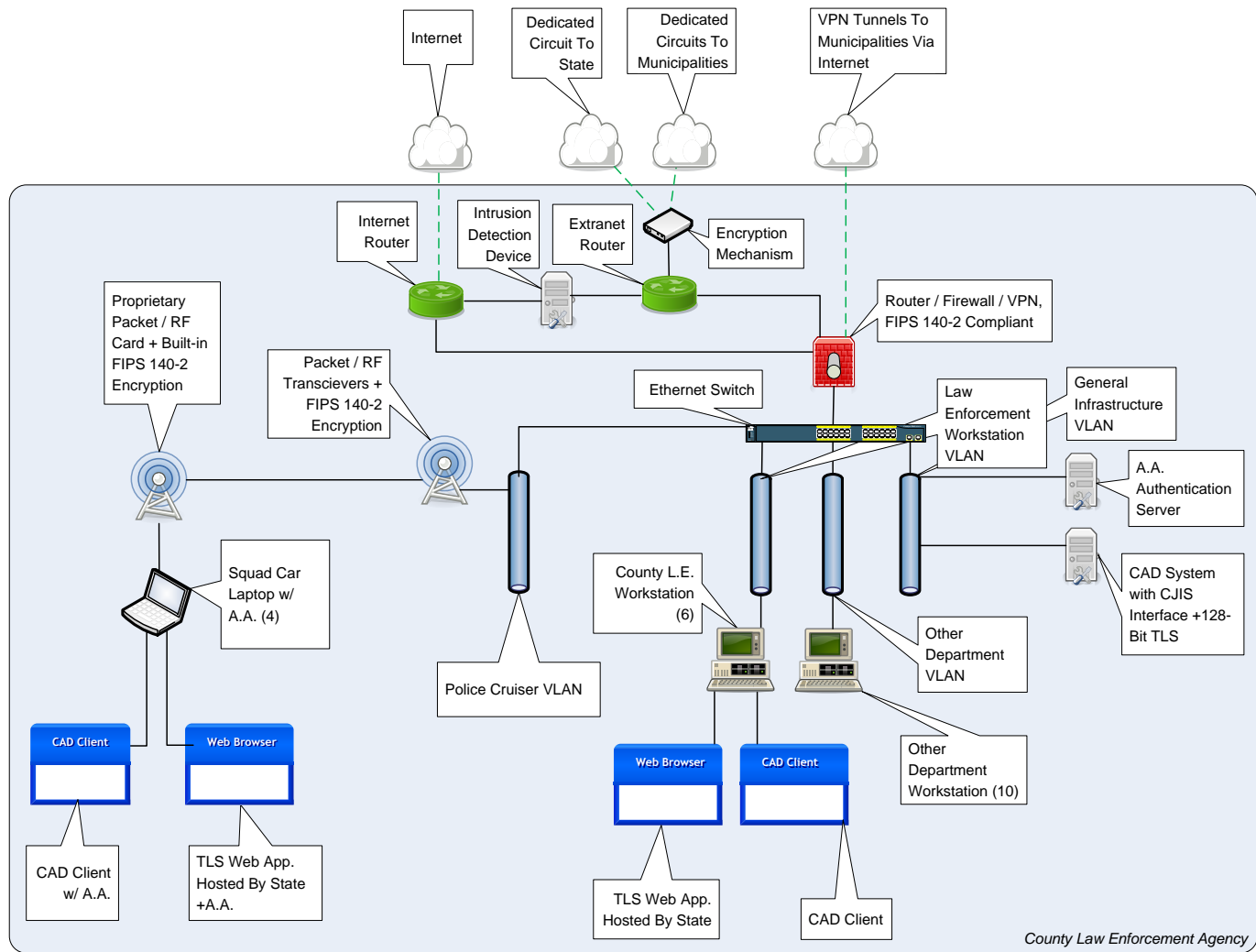
--- FIPS 140-2 COMPLIANT ENCRYPTION
 ——— STANDARD CONNECTION

Sample State Agency		
FOUO	01/01/2011	

Appendix C.1-B		
	01/01/2011	

Figure C-1-C Conceptual Topology Diagram for a County Law Enforcement Agency

Conceptual Topology Diagram For A County Law Enforcement Agency



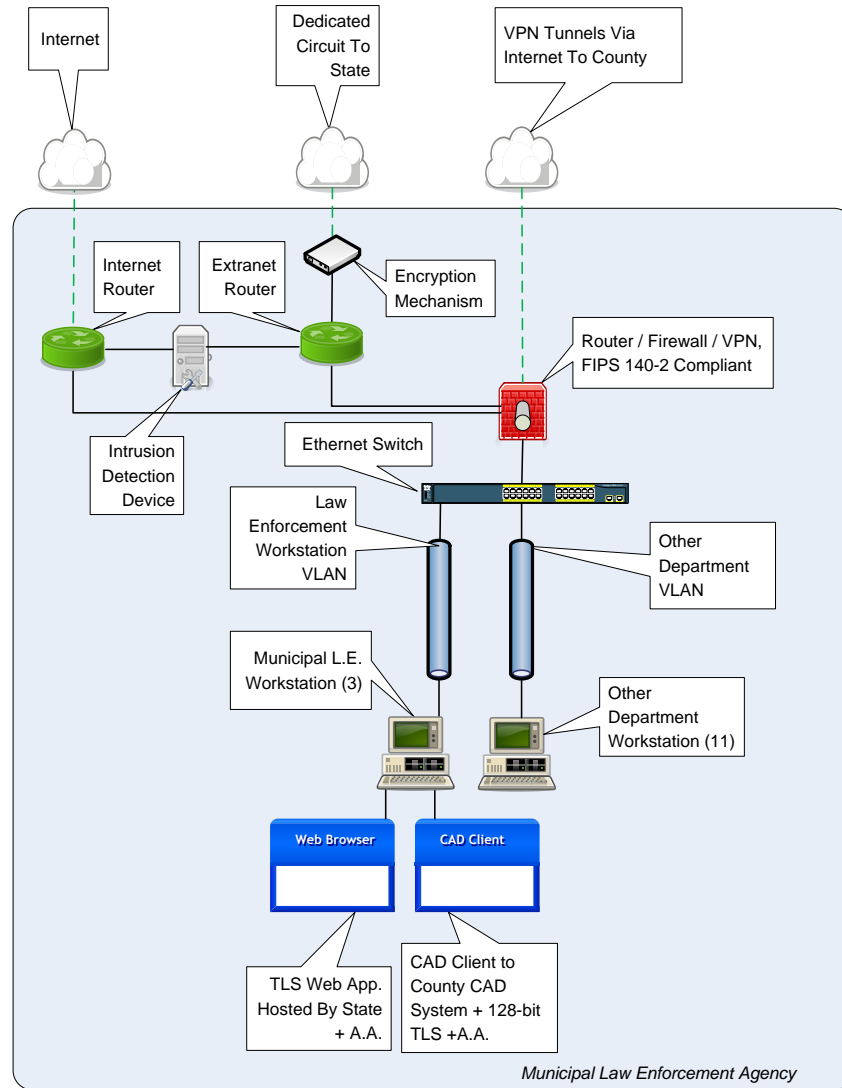
--- FIPS 140-2 COMPLIANT ENCRYPTION
 ——— STANDARD CONNECTION

Sample County Agency		
FOUO	01/01/2011	

Appendix C.1-C		
	01/01/2011	

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	

Appendix C.1-D		
	01/01/2011	

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 (III); 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 CJ. 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

_____ Date: _____
CJIS Systems Officer

Printed Name/Title

CONCURRENCE OF CSA HEAD:
_____ Date: _____
CSA Head

Printed Name/Title

PART 2

_____ Date: _____
CJIS WAN Official (or other CJIS Authorized Official)

Printed Name/Title

CONCURRENCE OF CJIS WAN AGENCY HEAD:
_____ Date: _____
CJIS WAN Agency Head

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.

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:

George White

(FBI CJIS Division ISO)
1000 Custer Hollow Road
Clarksburg, WV 26306-0102
(304) 625-5849
iso@ic.fbi.gov

John C. Weatherly

(FBI CJIS CSIRC POC)
1000 Custer Hollow Road/Module D-2
Clarksburg, WV 26306-0102
(304) 625-3660
iso@ic.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 announce 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.

REMEDICATION: 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.

REMEDICATION: 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.

REMEDICATION: 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.).

REMEDICATION: 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 CJI 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:

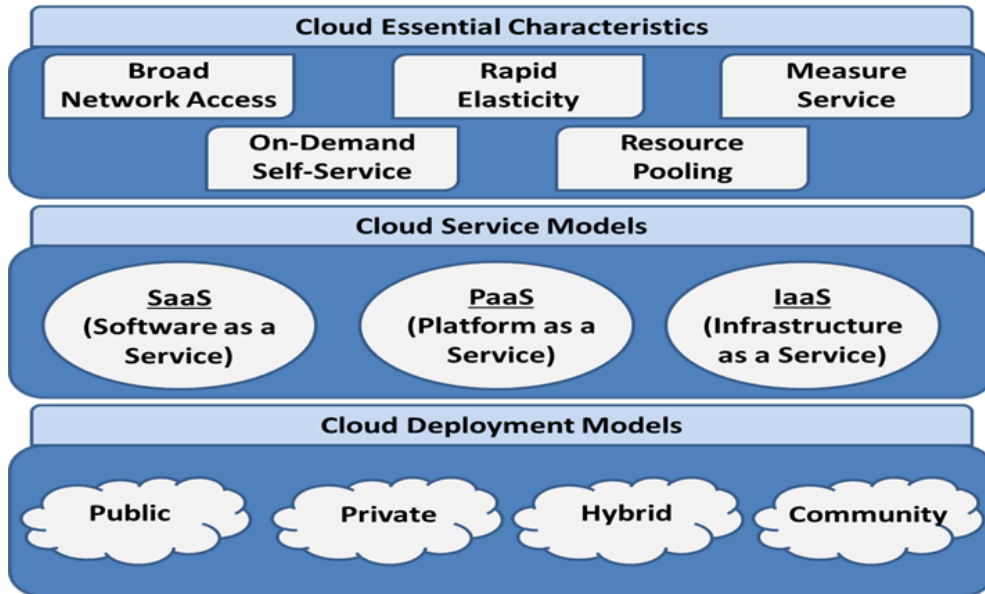


Figure 1 - Visual Depiction of the NIST Cloud Computing Definition

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 expenses 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.

- 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

- 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 reinstated in a timely and organized manner.

Incident Response

- 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 matter 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 system as 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.	<i>Quick win (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	<i>Quick win</i>
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.	<i>Quick win</i>

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).

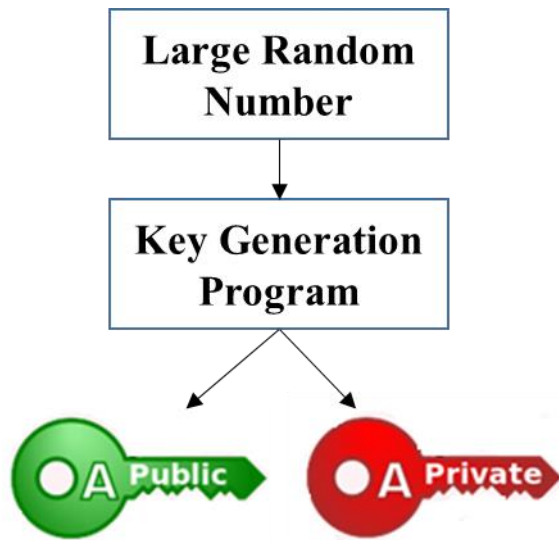


Figure 1 – Asymmetric key pair generation

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 #XXXX. <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.

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
- [DOJ Order 0904] *CYBERSECURITY PROGRAM*, Department of Justice (DOJ) Order 0904, September 15, 2016
- [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 per authorization of Department of Justice (DOJ) Order 0904.

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 CJJ 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 CJJ 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 CJJ 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 CJJ is processed. The CJJ 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 CJJ.

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 CJJ, 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 CJJ 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 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 access to CJI - listed in CSP Section 5.12.1.1. In addition to the requirements listed in CSP Section 5.12.1.1 contractors and vendors must undergo additional screening requirements as listed in CSP Section 5.12.1.2.2.

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 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 access to CJI - listed in CSP Section 5.12.1.1. In addition to the requirements listed in CSP Section 5.12.1.1 contractors and vendors must undergo additional screening requirements as listed in CSP Section 5.12.1.2.

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.

Empowered by Innovation

NEC

Western Identification Network, Inc

ABIS Replacement Project

WIN-33

WIN NIST Input and Output Device Implementation Guide

May 27, 2012



Document History

VERSION	DATE	DESCRIPTION
V1.0	May 27, 2012	Initial release.

Table of Contents

1	INTRODUCTION	1-1
2	LIVESCAN IMPLEMENTATION TASKS	2
2.1	PRE-IMPLEMENTATION TASKS	2
2.1.1	<i>Configure Network Connectivity (Refer to Attachment A for a diagram of a typical network configuration and Attachment B for the WIN Network Management and Security Policy).</i>	2
2.1.2	<i>Configure WIN Access (Refer to Attachments C or D for the appropriate Checklists to be completed and exchanged between the Livescan agency the State ID Bureau and WIN/NECAM).</i>	2
2.2	INSTALLATION & FINAL IMPLEMENTATION TASKS	3
2.3	CONFIGURE LIVESCAN FOR LAN CONNECTIVITY - <i>COORDINATE WITH LIVESCAN VENDOR AND LOCAL IT RESOURCES.</i>	3
2.4	ENSURE END-TO-END NETWORK CONNECTIVITY - <i>COORDINATE WITH LOCAL IT RESOURCES, STATE ID BUREAU/IT RESOURCES AND LIVESCAN VENDOR.</i>	3
2.5	TEST LIVESCAN SUBMISSIONS	3
3	WIN ELECTRONIC FINGERPRINT DATA FLOW	4
4	ESSENTIAL ELECTRONIC FINGERPRINT SUBMISSION REQUIREMENTS	5
4.1	ESSENTIAL FINGERPRINT RECORD FORMAT REQUIREMENTS	8
4.1.1	<i>Fingerprint Record Types</i>	8
4.2	WSQ COMPRESSION (500 PPI)	8
4.3	J2K COMPRESSION (1000 PPI)	9
4.3.1	<i>NIST Formatting</i>	9
4.3.2	<i>NIST Verification File</i>	10
4.4	COMMUNICATION PROTOCOL REQUIREMENTS	10
4.4.1	<i>Printing Requirements</i>	10
4.5	TYPE 1 LOGICAL RECORDS	11

4.5.1	<i>WIN Minimum Required Type 1 Data Elements – Refer to WIN EBTS for detailed description of record contents and format.</i>	11
4.6	TYPE 2 LOGICAL RECORDS	11
5	ATTACHMENTS	12
5.1	ATTACHMENT A – GENERIC REMOTE INPUT DEVICE NETWORK DIAGRAM & PORT ASSIGNMENTS	13
5.1.1	<i>Application Specifics</i>	14
5.1.2	<i>Specific List of TCP/UDP Ports</i>	15
5.2	ATTACHMENT B – WIN NETWORK MANAGEMENT AND SECURITY POLICY	16
5.2.1	<i>Introduction</i>	16
5.2.2	<i>Purpose</i>	18
5.2.3	<i>WIN status as a private entity:</i>	18
5.2.4	<i>Conclusion</i>	18
5.2.5	<i>Party Responsibilities</i>	18
5.2.6	<i>Applicability of the FBI-CJIS Security Policy</i>	19
5.2.7	<i>WIN Core Network Components</i>	19
5.2.8	<i>Recommended Network Management and Security Guidelines for WIN Members:</i>	20
5.3	ATTACHMENT C – AGENCY LIVESCAN INTERFACE TESTING PREPARATION CHECKLIST	27
5.3.1	<i>WIN Agency LS Interface Testing Preparation Checklist</i>	27
5.4	ATTACHMENT D – WIN AGENCY CCH INTERFACE TESTING PREPARATION CHECKLIST	30
5.4.1	<i>WIN Agency CCH Interface Testing Preparation Checklist</i>	30
5.5	ATTACHMENT E – WIN STANDARD FINGERPRINT CARD PRINT SPECIFICATIONS	32
5.5.1	<i>Text placement on Federal Criminal fingerprint (FD-249) card (8 inches x 8 inches pre-printed), front side:</i>	32
5.5.2	<i>Text placement on Federal Criminal fingerprint (FD-249) card (8 inches x 8 inches pre-printed), rear side:</i>	33
5.5.3	<i>Text and image placement on Federal Applicant fingerprint (FD-258) card (8 inches x 8 inches pre-printed), front (images) side only:</i>	34

5.5.4	<i>Text and Image Placement on NEC Verification Form (8.5 inches x 11 inches Template Printed) - Front Side Only</i>	35
5.5.5	<i>WIN Standard Template – Palm Print</i>	37
5.6	ATTACHMENT F – WIN MEMBER STATE FINGERPRINT CARD SPECIFICATIONS	39
5.6.1	<i>Alaska Fingerprint Card Print Specification</i>	39
5.6.2	<i>Alaska Fingerprint Card Print Specification</i>	40
5.6.3	<i>Alaska Fingerprint Card Print Specification</i>	41
5.6.4	<i>Alaska Specific Template – Palm Print</i>	42
5.6.5	<i>Idaho Specific Template - Applicant</i>	44
5.6.6	<i>Idaho Specific Template – Corrections Card - Front</i>	45
5.6.7	<i>Idaho Specific Template – Corrections Card - Rear</i>	46
5.6.8	<i>Oregon Specific Template – Criminal</i>	47
5.6.9	<i>Oregon Specific Template – Applicant</i>	49
5.6.10	<i>Oregon Specific Template – Palm Print</i>	50
5.6.11	<i>Text and image placement on WIN specific palm print form (8.5 inch x 11 inch page), front (images) side only – left palm:</i>	51
5.6.12	<i>Utah Specific Template – Criminal</i>	52
5.6.13	<i>Washington Specific Template – Criminal</i>	54
5.6.14	<i>Washington Specific Template – Department of Corrections Card</i>	56
5.6.15	<i>Washington Specific Template – Applicant</i>	58
5.6.16	<i>Washington Specific Template – Personal Identification</i>	59
5.6.17	<i>Washington Specific Template – Sex / Kidnapping Offender Registration</i>	60
5.7	ATTACHMENT G - PRINT SERVER SITE PREPARATION SPECIFICATIONS	62
5.7.1	<i>Power Requirements</i>	62
5.7.2	<i>Equipment Specifications</i>	62
5.7.3	<i>Network Requirement</i>	62
5.7.4	<i>Environment Required</i>	62
5.8	ATTACHMENT H – WIN MEMBER STATE FBI SUBMISSION ORI TABLE	63
5.8.1	<i>Attachment I - NEC AFIS Workstation and Associated Peripheral Equipment Installation Site Survey</i>	64
5.8.2	<i>Premises Wiring Color Code</i>	71

5.9	ATTACHMENT J – FBI IAFIS TENPRINT CONNECTIVITY CHECKLIST.....	73
5.9.1	<i>IAFIS Tenprint Connectivity Checklist.....</i>	73
5.10	ATTACHMENT K - FBI IAFIS LATENT CONNECTIVITY CHECKLIST.....	76
5.10.1	<i>Latent Connectivity Checklist.....</i>	76

List of Illustrations

Figure 5-1:	ABIS Devices Connected through State Owned Network	24
Figure 5-2:	ABIS Devices Connected through the Internet	25
Figure 5-3:	ABIS Devices Connected through 3 rd Party Vendor Encryption Service	26
Figure 5-4:	Ethernet T568B Color Diagram	71
Figure 5-5:	Network Diagram.....	72

List of Tables

Table 4-1 (ref 3-5)	FBI Compression Guidelines	5
Table 4-2 (ref 8)	ANSI-NIST ITL 2011 Guidelines	6
Table 4-3 (ref 8)	ANSI-NIST ITL 2011 Guidelines	7
Table 4-4	Network & Storage Comparison table 500 ppi vs. 1000	8
Table 4-5	Other additional record types sizes that should be considered	8
Table 4-6	Type 10 Mugshot/Scars Marks and Tattoos File size samples by level.....	9
Table 5-1	WIN ORI TABLE.....	63
Table 5-2:	Wiring Color Code	71
Table 5-3:	Ethernet Base - Patch Cord Colors	71

1 Introduction

The purpose of this document is to ensure the timely and successful implementation of a NIST qualified fingerprint input device interfaced to the WIN Automated Biometric Identification System (ABIS). Typically this will be a liveness or cardscan system. For simplicity, the term “liveness” will be used in this document to mean all NIST qualified fingerprint input devices.

In addition to liveness devices, the principals in this guide can be used for the implementation of interfaces to NIST Store & Forward and CCH servers. Checklist and preparation guides can be found in the attachments sections of this document. For a complete list of attachments, refer to Section 4 of this document.

With the exception of federal agencies the implementation of a liveness device and the subsequent submission of electronic fingerprints for processing to the WIN ABIS must meet the contributing agencies State Electronic Biometric Transmission Specification (EBTS). For a copy of a specific State’s EBTS, contact the specific State’s Criminal Identification Bureau.

All WIN member States fully comply with the current version of WIN EBTS, which in turn fully complies with FBI EBTS.

2 Livescan Implementation Tasks

To effect the implementation of a livescan system interfaced to the WIN system, the following tasks must be completed.

2.1 Pre-Implementation Tasks

2.1.1 Configure Network Connectivity (*Refer to Attachment A for a diagram of a typical network configuration and Attachment B for the WIN Network Management and Security Policy*).

1. Provide the State a dedicated IP address for each livescan device on the local subnet. Provided by livescan agency IT resources.
2. Coordinate configuration of WAN access to State's WIN State Workflow Manager (SWFM). Coordinate with State ID Bureau/IT resources.
3. Provide NAT and SMTP/FTP conduit on State router. Coordinate with State ID Bureau/IT resources.
4. Provide NAT and SMTP/FTP conduit on State's WIN Firewall. Coordinate with WIN Office and NLETS.

Note: At this point a conference call will be conducted with the principal parties from each affected entity to assure all requirements and timeframes are understood and agreed to. IP addresses, network port configurations, contact names, numbers, test schedules and procedures will be confirmed during this call.

2.1.2 Configure WIN Access (*Refer to Attachments C or D for the appropriate Checklists to be completed and exchanged between the Livescan agency the State ID Bureau and WIN/NECAM*).

1. Coordinate WIN access. Coordinate with State ID Bureau/IT resources, WIN and NECAM.
2. Create SMTP/FTP account on State WIN SWFM. Coordinate with State ID Bureau/IT resources, WIN and NECAM.

Note: Typically one to two weeks lead-time will be required to complete the pre-implementation tasks. However this could take longer depending on resource availability.

2.2 Installation & Final Implementation Tasks

1. Install livescan hardware, software and customized livescan management system. Coordinate with livescan vendor, local IT resources and State ID Bureau/IT resources.
2. Configure livescan SMTP/FTP submission interface components. Coordinate with livescan vendor, local IT resources and State ID Bureau/IT resources. Refer to Section 4 “Essential Electronic Fingerprint Submission Requirements”.
3. Provide local LAN connection for livescan. *Coordinate with local IT resources.*

2.3 Configure livescan for LAN connectivity - *Coordinate with livescan vendor and local IT resources.*

2.4 Ensure end-to-end network connectivity - *Coordinate with local IT resources, State ID Bureau/IT resources and livescan vendor.*

2.5 Test livescan submissions

1. Provide sample livescan NIST record for evaluation. *Provide to State ID Bureau, WIN and NECAM.*

Note: These samples will need to be provided at least 5 working days before the live tests are scheduled to begin.

2. Submit and track a small sample of live “test” transactions to the State WIN SWFM. Coordinate with livescan vendor, local IT resources, State ID Bureau/IT resources, NECAM and WIN.

Note: Livescan transactions may be submitted directly to the State WIN SWFM or to a State Store and Forward device that passes the transaction to the State WIN SWFM depending on configuration.

3. Sign off on live submission testing and schedule live production processing. *Coordinate with State ID Bureau.*

3 WIN Electronic Fingerprint Data Flow

Submission and processing of electronic fingerprint data is highlighted by the following steps:

Electronic fingerprint submissions will be sent to the State WIN SWFM. A livescan device will be configured to communicate with the State's WIN SWFM either directly or through a store and forward server.

The State WIN SWFM will route the transaction to the State Computerized Criminal History System (CCH). The CCH system will respond to the request from the State WIN SWFM.

The State WIN SWFM will communicate with the WIN Workflow Manager (WWFM). The WWFM will respond to the State WIN SWFM.

The WWFM will forward transactions to the FBI NGI and route NGI responses back to the State CCH.

4 Essential Electronic Fingerprint Submission Requirements

The WIN upgrade is strategically deploying central site components, which will be capable of passing through any valid NIST record type for storage on the central site NIST Archive System. Further clarification is necessary to make sure all members understand the capability that is being delivered as follows:

The upgrade is based upon member responses which confirmed all members intend to submit and process NIST Record Types 1, 2, 4 or 14 (fingers), and 15 (palm) optionally in 1000 ppi resolution.

All fingerprint and Palmprint images are to adhere to the following FBI compression guidelines taken from the FBI EBTS 9.3 Table 3-5.

Table 4-1 (ref 3-5) FBI Compression Guidelines

Ref: Table 3-5 Compression Algorithm Values

COMPRESSION ALGORITHM	BINARY VALUE	ASCII CODE
NONE USED (UNCOMPRESSED)	0	NONE
WAVELET SCALAR QUANTIZATION (WSQ) FBI REVISION 2.0	1	WSQ
JPEG ISO/IEC 10918 (LOSSY)	2	JPEGB
JPEC ISO/IEC 10918 (LOSSLESS)	3	JPEGL
JPEG 2K ISO/IEC 15444-1 (LOSSY)	4	JP2
JPEC 2K ISO/IEC 15444-1 (LOSSLESS)	5	JP2L
PORTABLE NETWORK GRAPHICS	6	PNG

Type 4 being up to 14 fingerprint images which includes up to 10 rolled images (fingers 1-10) plus four plain impressions (images 11-14) at 500 ppi resolution compressed using the FBI certified WSQ 15:1 compression methodology or: Type 14 being up to 14 fingerprint images captured at 500 ppi resolution compressed using the FBI certified WSQ 15:1 compression methodology or: captured at 1000 ppi compressed using JPEG 2K (JPL2) 10:1 compression methodology.

Type 14 record may be submitted as up to three “flat” impressions (indicated as fingers 13,14 &15) which will need to include the Segmentation Quality Metrics (SQM) or; up to 14 images that include 10 rolled images (1-10) plus four plain impressions (images 11-14).

If the type 14 is submitted as ten rolled images (fingers 1-10) plus four plain impressions (images 11-14), the images will be stored in the NIST Archive and forwarded onto the FBI as received. The WIN ABIS will process 500 ppi as well as 1000 ppi images.

The WWFM is to have capability to allow the State agency to select 500 ppi images as the default verification images. If the State agency network infrastructure is not able to support 1000 ppi image size, when the search generated candidates with 1000 ppi images, the WWFM is configured to send only the transcoded 500 ppi version of the images. It is anticipated that as the State agency network infrastructures are enhanced, more agencies will switch to reviewing 1000 ppi candidate images. The system permits the State agency system administrator to switch the default mode.

See the ANSI-NIST ITL 2011 finger position details.

Table 4-2 (ref 8) ANSI-NIST ITL 2011 Guidelines

Ref: Table 8 Friction ridge position code & recommended image dimensions Finger Positions Codes

FINGER POSITION	FINGER CODE	WIDTH		LENGTH	
		(MM)	(IN)	(MM)	(IN)
UNKNOWN	0	40.6	1.6	38.1	1.5
RIGHT THUMB	1	40.6	1.6	38.1	1.5
RIGHT INDEX FINGER	2	40.6	1.6	38.1	1.5
RIGHT MIDDLE FINGER	3	40.6	1.6	38.1	1.5
RIGHT RING FINGER	4	40.6	1.6	38.1	1.5
RIGHT LITTLE FINGER	5	40.6	1.6	38.1	1.5
LEFT THUMB	6	40.6	1.6	38.1	1.5
LEFT INDEX FINGER	7	40.6	1.6	38.1	1.5
LEFT MIDDLE FINGER	8	40.6	1.6	38.1	1.5
LEFT RING FINGER	9	40.6	1.6	38.1	1.5
LEFT LITTLE FINGER	10	40.6	1.6	38.1	1.5
PLAIN RIGHT THUMB	11	25.4	1.0	50.8	2.0
PLAIN LEFT THUMB	12	25.4	1.0	50.8	2.0
PLAIN RIGHT FOUR FINGERS (MAY INCLUDE EXTRA DIGITS)	13	81.3	3.2	76.2	3.0
PLAIN LEFT FOUR FINGERS (MAY INCLUDE EXTRA DIGITS)	14	81.3	3.2	76.2	3.0
LEFT & RIGHT THUMBS	15	81.3	3.2	76.2	3.0
RIGHT EXTRA DIGIT	16	40.6	1.6	38.1	1.5
LEFT EXTRA DIGIT	17	40.6	1.6	38.1	1.5
UNKNOWN FRICTION RIDGE	18	139.7	5.5	213.0	8.5
EJI OR TIP	19	114.3	4.5	127.0	5.0

Type 15 - being up to eight palm images captured at 500 ppi resolution compressed using the FBI certified WSQ 15:1 compression methodology or captured at 1000 ppi compressed using JPEG 2000 10:1 compression methodology. The palm print images must be accompanied by a set of corresponding fingerprints. The palm position codes from the following ANSI-NIST ITL 2011 Table 8 will be used to identify the palm position.

Table 4-3 (ref 8) ANSI-NIST ITL 2011 Guidelines

Table 8 Friction ridge position code & recommended image dimensions Palm Positions Codes

FINGER POSITION	FINGER CODE	WIDTH		LENGTH	
		(MM)	(IN)	(MM)	(IN)
UNKNOWN PALM	20	139.7	5.5	213.0	8.5
RIGHT FULL PALM	21	139.7	5.5	213.0	8.5
RIGHT WRITER'S PALM	22	44.5	1.8	127.0	5.0
LEFT FULL PALM	23	139.7	5.5	213.0	8.5
LEFT WRITER'S PALM	24	44.5	1.8	127.0	5.0
RIGHT LOWER PALM	25	139.7	5.5	139.7	5.5
RIGHT UPPER PALM	26	139.7	5.5	139.7	5.5
LEFT LOWER PALM	27	139.7	5.5	139.7	5.5
LEFT UPPER PALM	28	139.7	5.5	139.7	5.5
RIGHT OTHER	29	139.7	5.5	213.0	8.5
LEFT OTHER	30	139.7	5.5	213.0	8.5
RIGHT INTERDIGITAL	31	139.7	5.5	76.2	3.0
RIGHT THENAR	32	76.2	3.0	114.3	4.5
RIGHT HYPOTHENAR	33	76.2	3.0	114.3	4.5
LEFT INTERDIGITAL	34	139.7	5.5	76.2	3.0
LEFT THENAR	35	76.2	3.0	114.3	4.5
LEFT HYPOTHENAR	36	76.2	3.0	114.3	4.5
RIGHT GRASP	37	139.7	5.5	213.0	8.5
LEFT GRASP	38	139.7	5.5	213.0	8.5
RIGHT CARPAL DELTA AREA	81	139.7	5.5	114.3	4.5
LEFT CARPAL DELTA AREA	82	139.7	5.5	114.3	4.5
RIGHT FULL PALM, INCLUDING WRITER'S PALM	83	139.7	6.5	114.3	8.5
LEFT FULL PALM, INCLUDING WRITER'S PALM	84	139.7	6.5	114.3	8.5

Members may opt to submit additional NIST record types e.g. Type-7: documents; Type-8: Signature; Type-9: Minutia; Type-10: Mugshot/SMT, Type-16: developmental; Type-17: Iris; Type-18: DNA; Type-19: Plantar; Type-20: Source representation; Type-21: Associated Context; Type-98: Information Assurance and/or Type-99: CBEFF. Upon submission of these record types the system is functionally capable of processing and storing these record types. Users should coordinate with WIN if considering submission of these record types. There may be a need for additional network capacity to handle transmission of these additional record types and additional storage for NIST Archive.

4.1 Essential Fingerprint Record Format Requirements

4.1.1 Fingerprint Record Types

Per the WIN and FBI EBTS; each electronic fingerprint transaction will be comprised of one Type 1 “header” record, one Type 2 record and 1 to 14 Type 4/14 records (0-10 rolled fingerprint impressions and 4 sets of plain fingerprint, impressions). Flat submissions (4-4-2) are supported when submitted in Type-14 with FBI segmentation information required at capture.

4.2 WSQ Compression (500 ppi)

Type 4/14 logical records captured at 500 ppi must be compressed with the Wavelet Scalar Quantization (WSQ) algorithm, at an average compression ratio of 15:1 as specified in the WIN and FBI EBTS.

The following is a network and storage sizing chart that compares an average NIST compliant 14 image fingerprint record captured at 500 ppi with 15:1 WSQ compression (average 678 kb) to the variety of types of fingerprint submission sizes with and without palm print records at 500 and 1000 PPI capture rates.

Table 4-4 Network & Storage Comparison table 500 ppi vs. 1000

NIST RECORD SIZE FILE COMPARISONS	500 PPI CAPTURE WSQ 15:1	RATIO * : NN	1000 PPI CAPTURE J2K 10:1	RATIO * : NN
Type 1,2,4/14 (all 14 finger images)	680	1 : 1	4,720	1 : 6.9
Type 1,2,4/14 (1 Finger)	40	1 : 0.1	240	1 : 0.4
Type 1,2,4/14 (2 Finger)	80	1 : 0.1	480	1 : 0.7
Type 1,2,14 (Flats 4-4-2)	480	1 : 0.7	2880	1 : 4.2

Table 4-5 Other additional record types sizes that should be considered

RECORD TYPE	SIZE
Type 7 Document (300 ppi, 10:1)	1,152
Type 16 Test	Conditional
Type 17 Iris	Conditional

Table 4-6 Type 10 Mugshot/Scars Marks and Tattoos File size samples by level**Table 101: Example file sizes after compression**

LEVEL	MINIMUM WxH	UNCOMPRESSED SIZE (RGB888)	SIZE @ 2:1 LOSSLESS COMPRESSION	SIZE @ 15:1 COMPRESSION FOR THE ENTIRE IMAGE	SIZE @ 15:1 COMPRESSION FOR THE FACE AND 120:1 FOR THE BACKGROUND
30	480x600	844 KB		58 KB	19.34KB
40	768x1024	2.3 MB		156 KB	52.8KB
50	3300x4400	42.5 MB	14.2 MB		
51	2400x3200	22.5 MB	7.5 MB		

4.3 J2K Compression (1000 ppi)

WIN has adopted ANSI/NIST ITL 1-2011 record type definitions. Contained in these definitions is Type 14 – 1000 ppi resolution up to 14 image fingerprint records.

When 1000 ppi resolution image types are submitted, the NIST record size would increase from approximately 680 kilobytes to approximately 4.7 megabytes or more than 6 times the current 500 ppi record sizes. When palms are also submitted the 1000 ppi record could be up to 18 MB. Please see the WSQ vs J2K Comparison chart in Section 4.2.

If WIN members are considering capture, submission and storage of 1000 ppi resolution images, evaluation of network components and storage will need to take place otherwise overall production performance could be severely impacted. Until FBI NGI accept these records WIN Workflow Manager will transcode to 500 ppi before sending them.

If a member agency wishes to pass 1000 ppi Type 14/15 records through the WIN network and system and/or store these records on the WIN NIST Archive they must first contact the WIN office to discuss the impacts on WIN network, Archive and state SWFM systems.

In addition to the required 500 ppi capture, fingerprint images may be optionally captured at 1000 ppi at the Livescan and then transcoded to WSQ 10:1 compression using an FBI CJIS/NIST approved mechanism before submission to the state SWFM for ABIS processing (please reference FBI WSQ1000).

4.3.1 NIST Formatting

Electronic fingerprint transmissions will be comprised of NIST formatted data as specified in the WIN and FBI EBTS.

4.3.2 NIST Verification File

Each State will use a NIST verification file based on the FBI EBTS and WIN EBTS. However each State will have a customized NIST verification file specific to that States processing requirements that also encompasses the WIN and FBI specifications.

The current State NIST verification file should be obtained from your State ID Bureau/IT resources.

4.4 Communication Protocol Requirements

The communication protocols are detailed in the NEC/WIN Interface Design document. Please refer to “Section 3 - State CCH Interface” and “Section 2 - Input Device Interface”.

Note 1: Reference is made in the document to several RFC specifications. The full RFC specifications can be found on the Web at www.ietf.org/rfc.html.

4.4.1 Printing Requirements

Livescan devices that support fingerprint card printing must print using the WIN Member State’s print specification for any records being submitted to the state. This is a customized printing format utilizing the FBI criminal fingerprint card, FD-249 (REV. 5-11-99), the FBI applicant fingerprint card, FD-258 (REV. 12-29-82) and the States specification of use and printing position for the data elements. This custom specification should be obtained from the State ID bureau/IT resources.

Please see Attachment E for the “WIN Standard Fingerprint Card Print Specification”. Sample copies of current WIN States specific fingerprint cards specifications can be found in Attachment F.

4.5 Type 1 Logical Records

One Type 1 logical “header” record is required for each electronic fingerprint transaction/submission per the WIN and FBI EBTS and will be generated by the livescan device. Each state will have specifications for required data elements and content of the Type 1 records to be submitted to the SWFM. Contact the State ID Bureau/IT Resources for state requirements.

4.5.1 WIN Minimum Required Type 1 Data Elements – *Refer to WIN EBTS for detailed description of record contents and format.*

1. 1.01 - Logical Record Length (LEN)
2. 1.02 - Version (VER)
3. 1.03 – File Content (CNT)
4. 1.04 – Type of Transaction (TOT)
5. 1.05 – Date (DAT)
6. 1.06 – Transaction Priority (PRY)

Note: 1.06 is an optional field however, if the field is not populated the WIN Workflow Manager will default the priority to “9” which is the lowest priority. *Contact the State ID Bureau/IT Resources for the appropriate default priority for each particular livescan device.*

7. 1.07 – Destination Agency Identifier (DAI)

Note: Please refer to Attachment H for a list of ORI assignments for each WIN Member State.

8. 1.08 – Originating Agency Identifier (ORI)
9. 1.09 – Transaction Control Number (TCN)
- 10.1.11 – Native Scanning Resolution (NSR)
- 11.1.12 – Nominal Transmitting Resolution (NTR)

4.6 Type 2 Logical Records

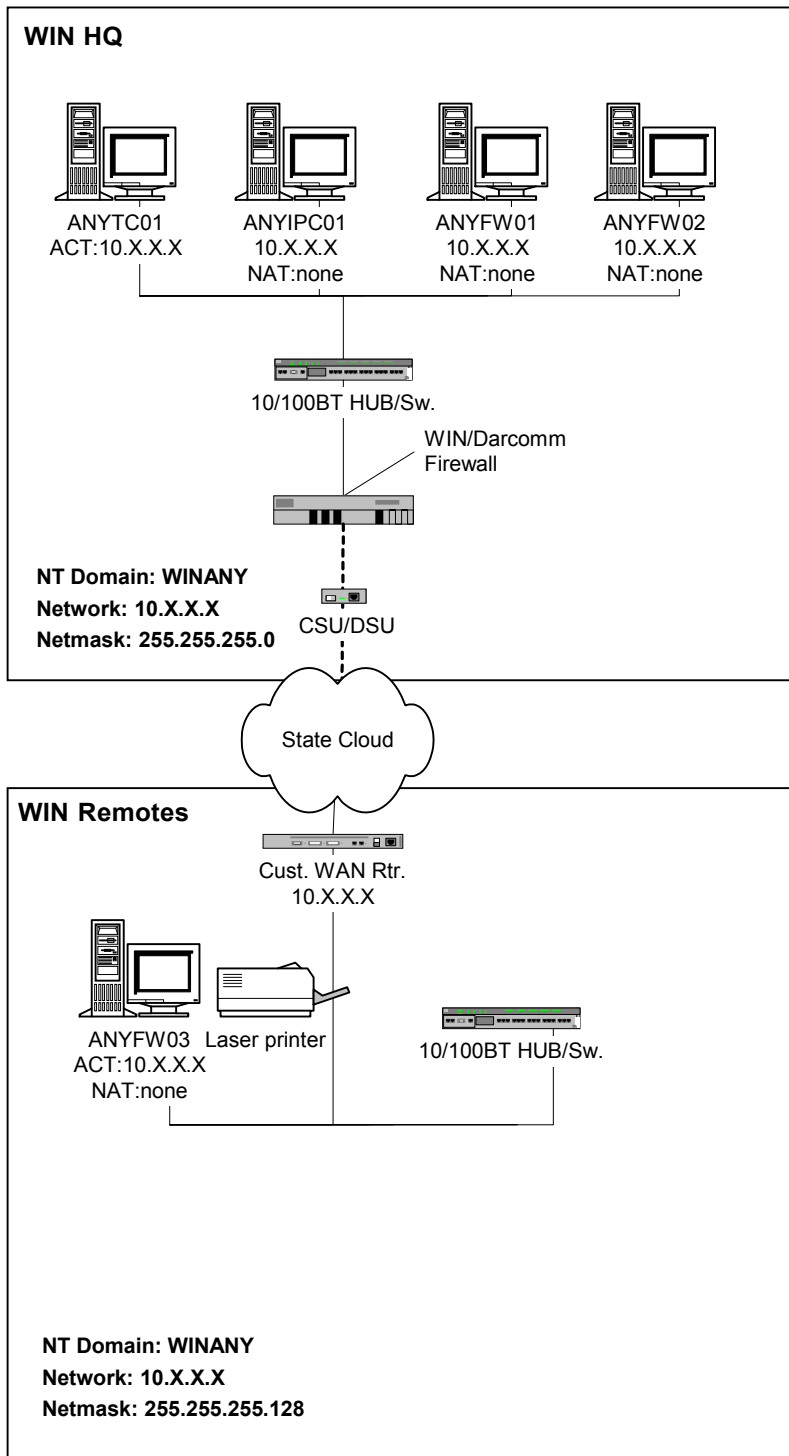
Each state’s electronic processing of Type 2 data elements includes mandatory and optional data elements defined in the WIN and FBI EBTS depending on the TOT of the record being submitted. *Coordinate with the State ID Bureau/IT Resources to determine state specific Type 2 data elements that are mandatory and optional for each type of livescan submission.*

5 Attachments

The following is a list of attachments included in this document.

- Attachment A Generic Remote Input Device Network Diagram and Port Assignments
- Attachment B WIN Network Management and Security Policy
- Attachment C Agency Livescan Interface Testing Preparation Checklist
- Attachment D WIN Agency CCH Interface Testing Preparation Checklist
- Attachment E WIN Standard Fingerprint Card Print Specifications
- Attachment F WIN Member State Fingerprint Card Specifications
- Attachment G Print Server Site Preparation Specifications
- Attachment H WIN Member State FBI Submission ORI Table
- Attachment I NECAM AFIS Workstation and Associated Peripheral Equipment Installation Site Survey
- Attachment J FBI IAFIS Tenprint Connectivity Checklist
- Attachment K FBI IAFIS Latent Connectivity Checklist

5.1 ATTACHMENT A – Generic Remote Input Device Network Diagram & Port Assignments



5.1.1 Application Specifics

*** Please use arrows as a guide for traffic direction

NEC ABIS application ports SWFM to iBW

ANYiBW ↔ ANYSWFM

10.X.X.X ← PING and TRACEROUTE mandatory

10.X.X.X → 20001 for initial application opening.

10.X.X.X → 1521 (AFIS application then uses RANDOM #'s)

10.X.X.X → HTTP (AFIS Archive Browser)

10.X.X.X → Application ports (random Oracle >1024)

10.X.X.X → FTP

10.X.X.X → POP3

10.X.X.X → netBios for DOMAIN auth.(possibly to be discontinued)

10.X.X.X → 53,1024-65535/TCP/UDP 53/TCP/UDP DNS

10.X.X.X → 1024-65535/TCP/UDP 88/TCP/UDP Kerberos

10.X.X.X → 1024-65535/TCP 445/TCP SMB

10.X.X.X ← PCAnywhere (ver. 9.0 ports 5631 TCP and 5632

Terminal Services (RDP 5.0) and Remote Desktop (RDP 5.1) is 3389.

10.X.X.X → PING using ICMP is mandatory for Active Directory to work.

10.X.X.X → Secure SNMP in future if available

ANYiBW ANYSWFM 10.X.X.X → 20002 (ULW Port)

5.1.2 Specific List of TCP/UDP Ports

Protocol	Port	TCP/UDP
DNS/DOMAIN	53	UDP/TCP
FTP	21	TCP
FTP Data	20	TCP
ICMP	ICMP	ICMP
Kerberos	88	UDP/TCP
MS Browsing	137	UDP
MS Browsing	138	UDP
MS Directory Replication	139	TCP
MS DNS Administration	135	TCP
MS DS Traffic/SMB	445	UCP/TCP
MS LDAP	389	UDP/TCP
MS NETBIOS-DGM	138	UDP
MS NETBIOS-SSN	139	UDP
MS Terminal Services	3389	TCP
pcanywhere-data	5631	TCP
pcanywhere-status	5632	UDP
POP3	110	TCP
Application Port Range	1024-65535	TCP
SMTP	25	TCP
SNMP	161	UDP
SNMP Trap	162	UDP
SSH	22	TCP

Port 80 needs to be open for Archive.

5.2 ATTACHMENT B – WIN Network Management and Security Policy

5.2.1 Introduction

This policy is intended to address areas of WIN responsibility and to recommend where best practices should be considered to implement responsive, secure and stable network facilities to support WIN.

WIN supports ABIS processing for eight western states. To accomplish this, WIN provides robust network facilities to the state identification bureaus in each of these states. WIN directly manages or indirectly facilitates connection of more than one hundred remote workstations, print servers, livescan, criminal history, and workflow interfaces.

To provide local flexibility and minimize cost while providing distributed ABIS services to state central sites and diverse remote locations, WIN has supported a cooperative network connectivity approach involving the WIN managed network, FBI-CJIS WAN and multiple state and local network domains.

WIN-ABIS performance is dependent on network availability, reliability, security and appropriate access managed and coordinated by WIN central site members within their respective states. The shared objective then is to:

- Provide appropriate network paths to all devices connected to WIN ABIS.
- Implement appropriate security to ensure integrity of data and limit access to those who need access.
- Recognize that state and local agencies are responsible for security policies with respect to their agency networks and facilities including compliance with CJIS security where applicable.
- Recognize that movement of arrest and civil applicant fingerprint and text data is sensitive information that is linked to criminal history and other state law enforcement information systems and must be protected appropriately.
- Recognize that to provide service levels requested by WIN members, all parties must work together to facilitate delivery of WIN ABIS services.
- Recognize that with the availability of today's firewall technology and related support tools, WIN and its members have the ability to secure the WIN network appropriately while allowing users and WIN service providers to do their jobs effectively and efficiently.

The cooperative network connectivity approach has been successful but does present challenges:

1. WIN is dependent upon its members and third parties who support WIN members to employ security and network practices consistent with industry standards that comply with the FBI-CJIS Security Policy as a minimum standard. This reliance is critical in that security of the broader WIN network community is dependent upon all parties doing a proper job of securing their networks.
2. No single entity is responsible for end to end telecommunications, related security, monitoring and management for remote devices. Accordingly, in some instances, WIN still does not have visibility to monitor the status of WIN managed and other remote devices that submit to WIN. WIN is dependent upon state and local agencies to be available to support device configuration, issue identification and resolution in these instances.
3. Each agency involved maintains their own access policies, standards and performance requirements for their networks and installed network devices.
 - WIN-ABIS devices are often connected to shared networks. The remote ABIS device competes for network capacity with other agency applications. Where these conditions are encountered, device performance can be impacted if bandwidth is not sufficient to support these combined application transport requirements.
 - Agency management for each network domain independently performs maintenance on their respective network involving changes to IP address and routing schemes, ports and other matters. These changes have periodically shut off connectivity of WIN connected devices that communicate from these networks.
 - WIN has found in some instances that encryption has not been employed where there is exposure to the INTERNET/Public Carrier or other non-law enforcement networks thus allowing a data integrity-security weakness to exist.
 - WIN has found that in some instances, member agencies have deployed network devices which are not suitable for the purpose they are being used. This contributes to degraded or unstable network and device performance.
 - WIN has observed device outages caused by local network outages which have not been communicated to the user. Accordingly, the user looks to WIN to resolve when the corrective action needed is to restore the local network.
4. Agency representatives who are actively involved in WIN do not necessarily have access or provide policy or operational direction to agency network managers. Agency network managers in some instances do not understand WIN's role with the State ID Bureau or the relationship of WIN managed latent workstations and other devices located at forensic sites.
5. It is not broadly understood that WIN is a qualified private entity authorized to provide services to criminal justice agencies under Title 28 C.F.R. and is subject to the FBI-CJIS Security Policy. Accordingly, WIN should be treated as a trusted partner that is subject to the same rules for network security as all law enforcement agencies who

participate in the FBI-CJIS WAN. WIN is similar to NLETS though a smaller network footprint dedicated to connection with WIN -AFIS.

5.2.2 Purpose

This policy is intended to explain the WIN Network environment and discuss placement of points of demarcation to attribute responsibility for management and security of the network among the involved parties, WIN, state, local, FBI-CJIS, NECAM, NLETS.

5.2.3 WIN status as a private entity:

WIN is a private entity operating in compliance with USDOJ rules contained in Title 28 of the Code of Federal Regulations (C.F.R.). Accordingly, WIN is authorized to provide services to criminal justice agencies pursuant to this agreement. Such an agreement is the CJIS Security Addendum.

1. WIN has executed a security addendum with each WIN Central Site Member.
2. WIN has executed a security addendum with WIN third party service providers (e.g. NECAM, NLETS).
3. WIN and involved third parties are fingerprinted and criminal history background checked.
4. WIN is subject to audit per provisions of the CJIS security addendum.
5. WIN is subject to compliance with the FBI-CJIS Security Policy.

5.2.4 Conclusion

WIN is positioned to provide services to criminal justice agencies and should generally be viewed as a criminal justice partner for the defined purpose of delivering ABIS services and managing related network security issues associated with WIN User Agreements. Though for a narrower more restrictive ABIS purpose, WIN operates similarly to NLETS in this respect. Both organizations are private non-profits operating under USDOJ regulations allowing them to provide these services.

5.2.5 Party Responsibilities

- **WIN** - WIN is responsible for providing the core network from the WIN central site to each State Identification Bureau and for maintaining the WIN - CJIS WAN and proprietary NECAM ESSO gateways. The demarcation point for handing off network responsibility to the state central sites is the state SWFM unless specifically expanded by an amended user agreement with WIN.
- **STATE** - WIN State Central Sites are responsible for provision of network facilities from the SWFM to state and local sites.

WIN Members are responsible for security behind their firewalls and to configure their network components which support AFIS related traffic in a manner consistent with the WIN NIST device configuration guide and WIN Security Policy. WIN has adopted by reference, the FBI-CJIS Security Policy.

1. WIN performance is dependent on the state and local portion of the networks and facilities managed by them. If contracted levels of service are desired, state and local environments need to enable this.
2. WIN Central Site Members are responsible for notifying and coordinating network changes that will impact WIN connected devices to ensure continued device connectivity.

NECAM - NECAM Responsibility is to maintain and otherwise support hardware and software necessary to deliver contracted AFIS services. This is primarily understood as the ABIS application.

NLETS - NLETS responsibility is to manage the WIN Network. This is understood as the transport layer and primarily involves management of the core WIN managed network components (e.g. MPLS and routers).

5.2.6 Applicability of the FBI-CJIS Security Policy

1. WIN Maintains a CJIS WAN Gateway and is subject to USDOJ regulations. Accordingly, WIN is subject to the FBI-CJIS Security Policy for these purposes.
2. WIN has signed CJIS security addendums with each State Central Site Member thus subjecting WIN to compliance with the FBI-CJIS Security Policy.
3. WIN States have signed a User Agreement with WIN indicating that members will comply with the FBI-CJIS Security Policy and other security practices adopted by WIN.
4. The WIN Board approved a motion that WIN members shall treat devices that submit, communicate, interface or are otherwise connected to WIN, shall be secured in a manner consistent with policies, methods and procedures contained in the FBI-CJIS Security Policy regardless of whether data being passed, queried, or updated is FBI-CJIS data.
5. The discussion leading to the motion recognized that WIN requires a security policy. The Board concluded that since the FBI-CJIS Security Policy is broadly understood and that national resources are already committed to maintaining the policy, it makes sense for WIN to adopt the FBI-CJIS Security Policy rather than expending WIN resources to develop and maintain its own separate security policy.

5.2.7 WIN Core Network Components

1. WIN provided network components are firewalled by the use of CISCO routers and are VPN encrypted from the WIN Central Site to each State Central Site.

NLETS provides monitoring, problem resolution and configuration support 7 X 24.

2. WIN – NECAM – NLETS operate within the requirements of the FBI-CJIS Security Addendum which includes a requirement to comply with the FBI-CJIS Security Policy.

5.2.8 Recommended Network Management and Security Guidelines for WIN Members:

It is not our intent to detail or repeat content contained in the FBI-CJIS Security Policy or the WIN NIST Device Configuration Guide. These sources are considered key references for members seeking guidance on how to install, secure and use devices connected to WIN. The following discussion points represent issues that WIN frequently encounters that can help provide focus to members in their effort to deploy, manage and secure devices connected directly or indirectly to WIN:

1. **Educate Your State and Local Agency Network Personnel what WIN is** –The greater the level of understanding and trust established with network personnel, will tend to allow WIN more efficient and effective access to support the WIN devices in your state.
2. **Educate Your State and Local Users To Differentiate WIN supplied and managed components from agency maintained components at their location** – It can save response time and reduce user frustration if the user has a basic understanding of the components the user is dependent upon and have a local contact to help determine if there is a local issue causing a problem.
3. **Educate Your State and Local Network Managers to be aware of WIN connected devices within the context of making modifications to networks and firewalls from which WIN devices communicate.** To the extent WIN devices are considered during network changes, will facilitate notification to WIN so that required configuration changes on the WIN side can be anticipated, planned for and implemented without unduly disrupting user service.
4. **Educate Your State and Local Agencies that to enable WIN to be responsive to them and also be cost effective, WIN Service Providers require network and remote dial-up access to support WIN-ABIS and related components submitting to WIN from their networks** – Given that WIN and its service providers, NECAM and NLETS are subject to CJIS Security Policies and that modern network firewall technology can restrict WIN Service providers to a specific device, specific ports, types of traffic and permissions, WIN believes that state and local agency security concerns can be addressed in a manner that enables proper remote support of WIN connected devices.
5. **Include Security Requirements in Contracts** – Agencies who procure livescan and other devices that will capture or submit to WIN need to address anti-virus, remote maintenance, firewall and configuration management to lock down devices and users of the devices for authorized purposes.
 - Reference WIN NIST Device Configuration Guide
 - Reference FBI-CJIS Security Policy
6. The INTERNET (Reference FBI-CJIS Security Policy version 5.0, sec 5.10)

7. Mitigate Exposure to the Public Internet – Law enforcement applications will use modern software that employs internet tools but this does not necessarily mean that applications will operate on the public internet. Modern INTERNET software is often deployed on private networks in support of internal agency/corporate applications. To the extent feasible, devices ultimately submitting data or queries to WIN should avoid use of the public internet.
8. Given that modern technology uses operating systems, software and hardware that have robust internet enabled tools, modern application systems take advantage of these tools that require routers to be configured to allow this type of traffic. This traffic is being secured with effective use of firewalls and encryption to appropriately restrict access.
9. Where devices must transit the public INTERNET/Public Carrier, encryption is required to guarantee data integrity. Depending on the nature of the traffic and use, encryption can be accomplished by creating a dedicated virtual private network (VPN) tunnel or by use of Secure Socket Layer (SSL) encryption.
 - For dedicated devices (e.g. Latent Workstations, Store and Forwards, Print Servers), a dedicated VPN tunnel is recommended to provide the level of encryption needed and this configuration also facilitates device support from a troubleshooting standpoint. A VPN tunnel is established by connecting an encryption device e.g. CISCO 5505, 501 to the dedicated WIN component.
 - For non-dedicated devices such as, livescans, SSL is acceptable and tends to be a more cost effective method of securing large numbers of these devices. Uses of SSL concentrators such as those provided by Juniper Systems are helpful to connect, encrypt, and manage multiple devices. These devices have additional capabilities that will verify the antivirus software on connected devices is present and current or the device will not let traffic through.
10. **Document Archive Access** – WIN members should avoid use of Public IP addresses for receiving Archive responses. Agencies should configure these responses so that they transit on secure law enforcement network routes. This can be accomplished by employing a switch from the WIN ASA router and connecting with cables. NLETS will supply a diagram to facilitate this configuration.
11. Device Management –
12. **Allow PING and TRACEROUTE Access to Device** - WIN members need to secure internal agency support to allow WIN ICMP (PING) access to WIN connected devices in their states. This enables several benefits that are not universally available now including:
 - NLETS can poll ping enabled devices to confirm they are visible on the network. If a device is not visible, designated individuals can be notified automatically by email or page.
 - This provides the first step in active management of the devices and can report some device problems before a problem ticket needs to be generated.
 - Facilitates identification of network outages along device routes.

13. **Allow PC Anywhere Dial-Up Access to WIN supported devices** –(Reference FBI-CJIS Security Policy 5.0, Section 5). When there is a need to update software on a device, troubleshoot a problem reported by a user, dial-up access is an essential tool. This capability facilitates timely cost effective device support.
14. **WIN Managed Encryption Services (VPN-SSL)** – Through NLETS, WIN can provide SSL managed services. In addition to the benefits achieved from PING access, WIN would encrypt all devices submitting to the state central site and monitor to ensure connected devices have current virus scan software. This service will protect state and WIN security interests.
15. **WIN Member Managed Encryption (VPN-SSL) Services** - Members may acquire and manage their own encryption equipment, but if they choose to do so, WIN can only monitor the network and assist with troubleshooting to the point the WIN network visibility terminates. If visibility terminates at the State Global Transaction Controller, WIN will be dependent upon State and Local network administrators to resolve network issues prior to NECAM being able to successfully provide diagnostic support. At times in the past, this becomes very time consuming and frustrating for end point users. We have found where WIN has had end to end visibility; remote device support tends to be more efficient and effective.

Agencies that purchase their own 5505 or similar concentrator will need to work with WIN and NLETS to set up the Peer IP Address and basic configuration on the device. All other set up requirements will be the responsibility of the individual agency and or state network personnel. Following is the set up specifications that would be provided by NLETS.

- Peer IP Address - IP addresses/IP Networks that are allowed to communicate over the VPN tunnel
- Phase 1 Configuration
 - Authentication Pre-Shared Key
 - Hash MD5 (minimum)
 - Lifetime 86400
 - Encryption 3des (minimum)
 - Diffie-Hellman Group 2 (minimum)
- Phase 2 Configuration
 - Transform - Set esp-3des esp-md5-hmac (minimum)
 - Basic testing across the VPN tunnel to establish connectivity, Ping, Trace-Route, etc
- **WIN Supplemental Network Services** – In the event a member determines it is more appropriate, WIN can provide supplemental network services through NLETS as an amendment to the user agreement.
- **Anti-Virus Software** – Anti-virus software needs to be present on all application servers and workstations and maintained on a current basis.

-
16. **Virtual LAN Configurations** – V-Lans can be appropriate configurations provided suitable higher end routers and switches are in place to enable proper support for this type of configuration.
 17. **State and Local managed network components need to be appropriate and monitored** – To ensure reliability, speed and functionality WIN recommends that members carefully review the capability of local switches, hubs and other components they are utilizing as part of the connection of devices to WIN to verify these components are appropriate for the type and volume of traffic intended.
 18. **Store and Forward Technology** – Use of store and forwards to serve as livescan consolidators is appropriate to facilitate connection of multiple livescans with one SWFM connection.

Figure 5-1: ABIS Devices Connected through State Owned Network

AFIS Devices Connected via State Owned Network

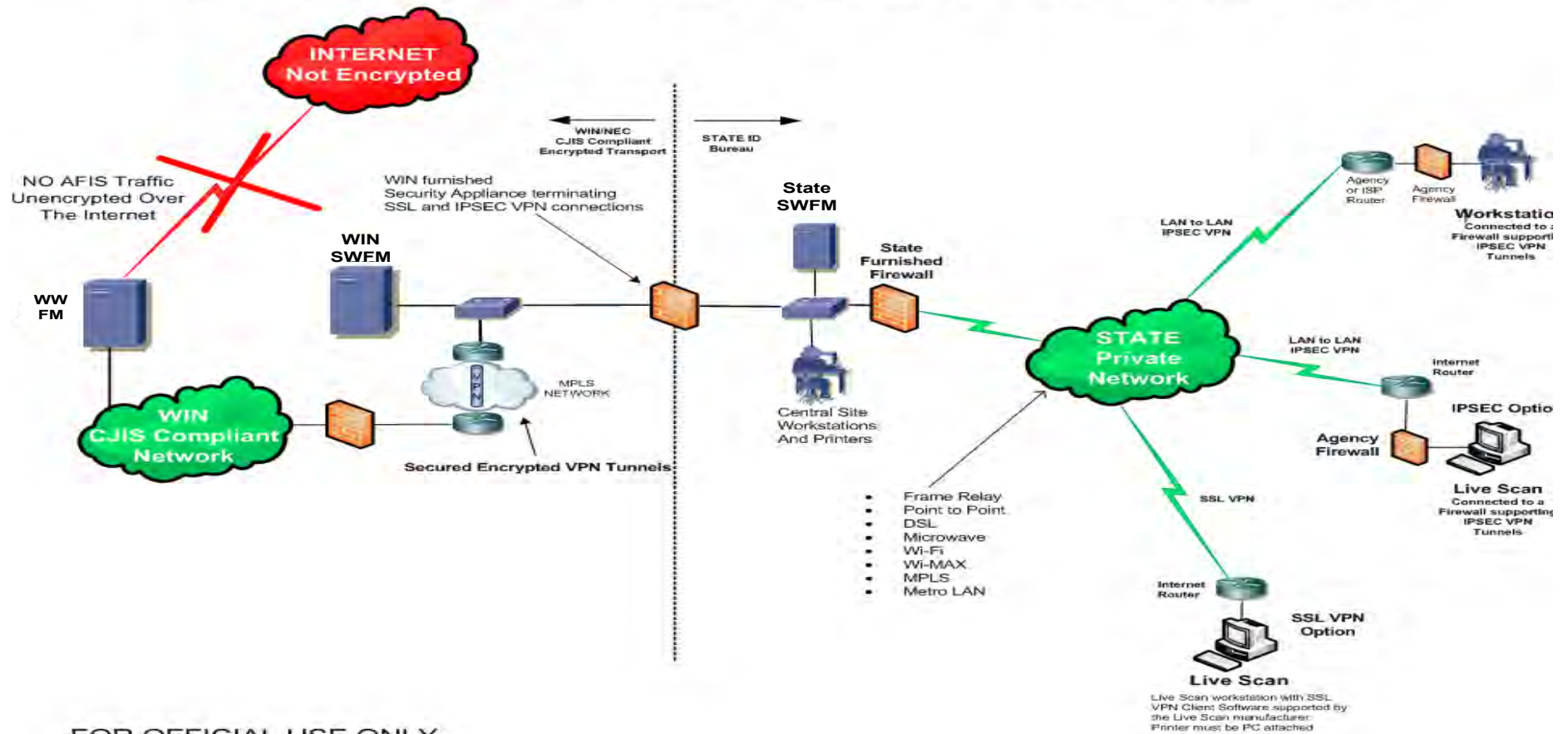
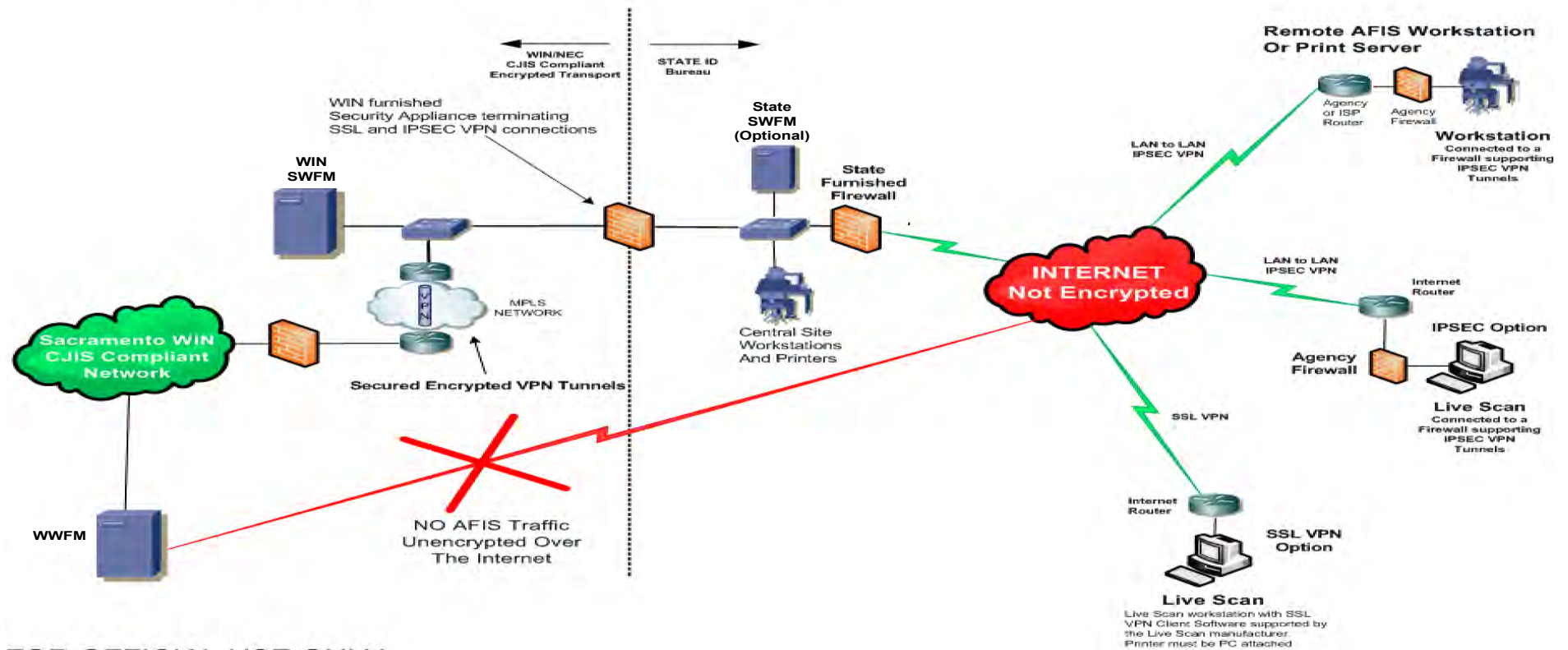


Figure 5-2: ABIS Devices Connected through the Internet

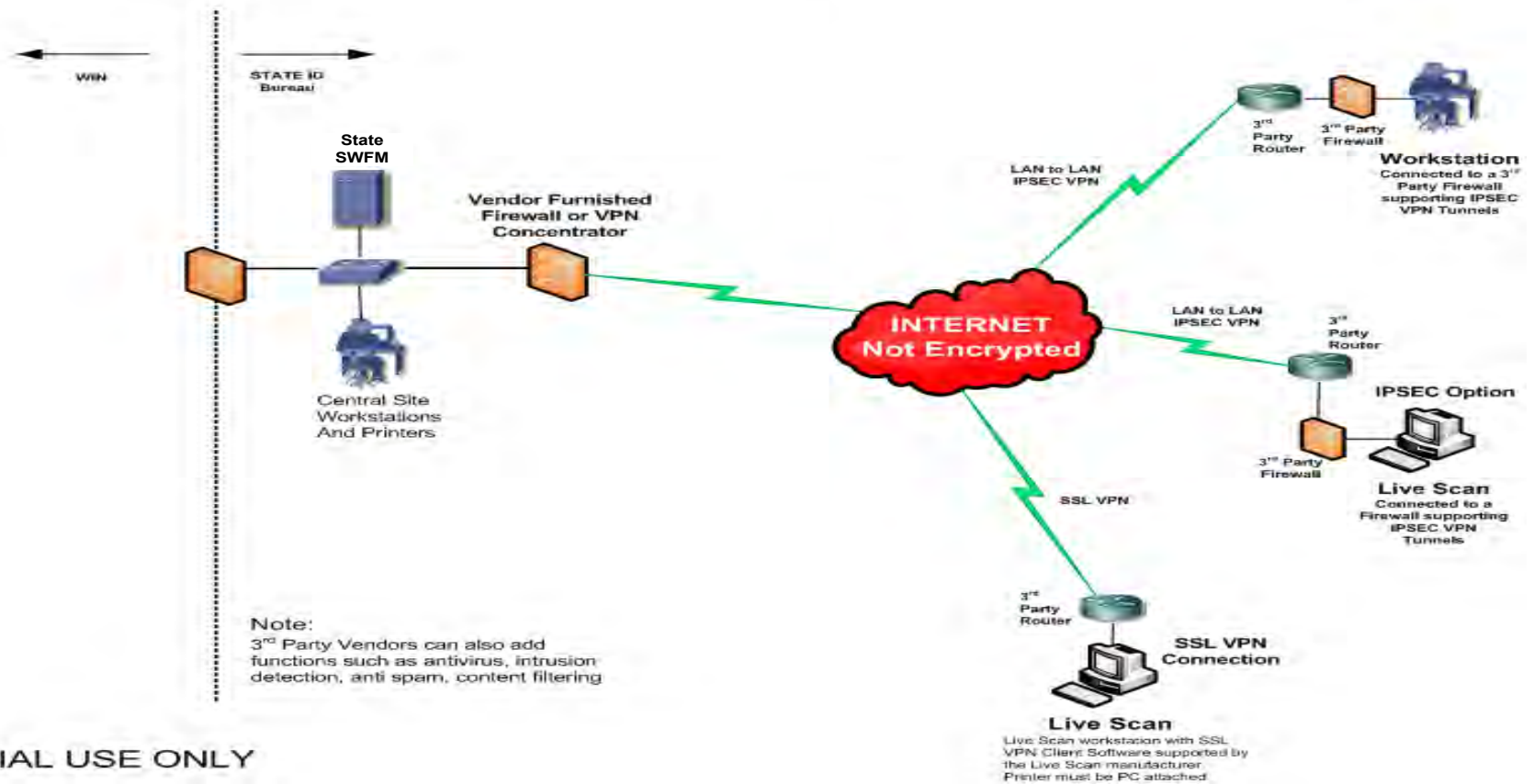
AFIS Devices Connected via Internet



FOR OFFICIAL USE ONLY

Figure 5-3: ABIS Devices Connected through 3rd Party Vendor Encryption Service

AFIS Devices Connected via 3rd Party Vendor ENCRYPTION Service



5.3 Attachment C – Agency Livescan Interface Testing Preparation Checklist

5.3.1 WIN Agency LS Interface Testing Preparation Checklist

Information provided by Agency and BCI and Vendor

Livescan Agency: PD/SO etc

1. Please describe below how the device will be installed to meet WIN and FBI/CJIS Network Management and Security Policy. _____

2. Please provide the e-mail address for your State Livescan Server: _____

Example: sttc01@sttc01.winafis.org (State SWFM)

3. Will this be a direct connection? _____

4. Will this device connect through a Store & Forward Server? _____

5. Please provide the IP address for your State Livescan Server: _____

Example: 123.123.123.123

6. Please provide a list of contact names with phone number and e-mail address along with title and area of responsibility for each person from your agency that WIN and NECAM personnel should work with on this project.

Livescan Agency Contacts

Example:

Sgt. Jane Doe 555-123-4567
jdoe@metropd.state.gov

Susan Smith 555-123-8910
ssmith@metropd.state.gov

Vendor Contacts

Georgette Vendor 555-333-7777
georgette.gregg@identix.com

7. Please state the anticipated timeframe for testing and implementation.

Testing: **Starting November 1, 2009**_____

Implementation: **November 14, 2009**_____

8. Please provide the number of devices being installed, the IP address assigned to each device, and the anticipated daily/hourly throughput per device._____

Example: 168.111.222.333 - Livescan IP 168.222.444.888 – Printer/transmitter

9. State ID Bureau Contacts

Example: Alice Johnson
 Manager
 (555) 999-4444
ajohnson@state.gov

Chris Craft
 Network Administrator
 (555) 222-5555
ccraft@state.gov

Information Provided by WIN & NEC

1. What is the e-mail address for the State SWFM? sttc01@sttc01.winafis.org_____
2. What is the IP address for the State SWFM? 168.123.456.789_____
3. Please provide a list of contact names with phone numbers and e-mail addresses for persons from WIN and NEC that state personnel should work with on this project.

WIN Contacts

Gary Goad

Member Services Manager

(916) 369-3946 ext 223

gary@winid.org

Dusty Clark

Training & Quality Assurance Specialist

(916) 369-3946 ext 230

dusty@winid.org

NEC Contacts

Jim Riddle

Systems Engineer

(916) 463-7074

jimmy.riddle@NECAM.com

Please reference the WIN Interface Design Document, CDRL Win-14, Section 2 “Input Device Interface”.

Please confirm/verify NIST record creation conforms to all related specifications and standards. WIN and User agency should check NIST formatting before sending to State Agency.

SYNOPSIS of CONFIGURATION details given for this device:

Input Device ID: **IDXxxx**

Input Device Group ID:

002 Input=FTP

Output=SMTP

To=**idxXXX@STTC01**

Atn=**STIDXxxx**

Err=**idxXXX@STTC01**

Unique password for the device:

stidxXX Outbox for responses:

idxXXX@STTC01

ATN assigned to ALL devices: **STIDXxxx** (Please ensure 2.006 field has a value in it though)

TCP/IP address: **168.123.456.789**

Host Name:

sttc01@sttc01.winafis.org

SUBJECT is not needed for SMTP submission.

5.4 Attachment D – WIN Agency CCH Interface Testing Preparation Checklist

5.4.1 WIN Agency CCH Interface Testing Preparation Checklist

Information Provided By CCH Agency

CCH Agency: _____

1. Please provide the e-mail address for your State CCH Server.

2. Please provide the IP address for your State CCH Server

3. Please provide a list of contact names with phone number and e-mail address along with their title and area of responsibility for each person from your agency WIN and NECAM personnel should work with on this project.

4. Please state the anticipated timeframe for testing and implementation.

Testing: _____

Implementation: _____

Information Provided By WIN & NECAM

1. What is the e-mail address for the State SWFM? _____

2. What is the IP address for the State SWFM? _____

3. Please provide a list of contact names with phone numbers and e-mail addresses for persons from WIN and NEC that state personnel should work with on this project.

WIN Contacts

Gary Goad

Member Services Manager

(916) 369-3946 ext 223

gary@winid.org

NEC Contacts

Jim Riddle

Systems Engineer

(916) 463-7074

jimmy.riddle@NECAM.com

Dusty Clark

Training & Quality Assurance Specialist

(916) 369-3946 ext 230

dusty@winid.org

5.5 Attachment E – WIN Standard Fingerprint Card Print Specifications

5.5.1 Text placement on Federal Criminal fingerprint (FD-249) card (8 inches x 8 inches pre-printed), front side:

LEAVE BLANK CRIMINAL SID:[2.015 #1]		(STAPLE HERE) <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <small>NFF SECOND SUBMISSION APPROXIMATE CLASS AMPUTATION SCAR</small>			LEAVE BLANK			
STATE USAGE CASE-NUM: [2.934] TCN:[1.09]		LAST NAME, FIRST NAME, MIDDLE NAME, SUFFIX [2.018] [2.908.1][2.908.2" "[2.908.3" "[2.908.4" "] #1						
SIGNATURE OF PERSON FINGERPRINTED		SOCIAL SECURITY NO. [2.016 #1] [2.016 #2]		LEAVE BLANK				
ALIASES/MAIDEN LAST NAME, FIRST NAME, MIDDLE NAME, SUFFIX [2.019 #1] [2.908.1][2.908.2" "[2.908.3" "[2.908.4" "] #2 [2.019 #2] [2.908.1][2.908.2" "[2.908.3" "[2.908.4" "] #3								
FBI NO. [2.014#1]	STATE IDENTIFICATION NO. [2.015#1]	DATE OF BIRTH MM DD YY [2.022#1]	SEX [2.024]	RACE [2.025]	HEIGHT [2.027]	WEIGHT [2.029]	EYES [2.031]	HAIR [2.032]
[2.084]/[2.124.2] #1	[2.084]/[2.124.2] #2	[2.084]/[2.124.2] #3	[2.084]/[2.124.2] #4		[2.084]/[2.124.2] #5			
[H.RT]	[H.RI]	[H.RM]	[H.RR]		[H.RL]			
1. R. THUMB	2. R. INDEX	3. R. MIDDLE	4. R. RING		5. R. LITTLE			
[2.084]/[2.124.2] #6	[2.084]/[2.124.2] #7	[2.084]/[2.124.2] #8	[2.084]/[2.124.2] #9		[2.084]/[2.124.2] #10			
[H.LT]	[H.LI]	[H.LM]	[H.LR]		[H.LL]			
6. L. THUMB	7. L. INDEX	8. L. MIDDLE	9. L. RING		10. L. LITTLE			
[2.067.1][2.067.2] SCANNER ID	[2.067.3] SCANNER S/N	[2.038] [2.481]	[Current PRINTER S/N] (Actual Printer, Not Stored)		[Current DATE:TIME]			
[H.L4]		[H.LTP]	[H.RTP]	[H.R4]				
LEFT FOUR FINGERS TAKEN SIMULTANEOUSLY		L THUMB	R THUMB	RIGHT FOUR FINGERS TAKEN SIMULTANEOUSLY				

5.5.2 Text placement on Federal Criminal fingerprint (FD-249) card (8 inches x 8 inches pre-printed), rear side:

FEDERAL BUREAU OF INVESTIGATION, UNITED STATES DEPARTMENT OF JUSTICE WASHINGTON, D.C. 20537				SID: [2.015 #1]
<small>PRIVACY ACT OF 1974 (5 U.S.C. 552a) AND FEDERAL BUREAU OF INVESTIGATION (44 CFR 1.562) REQUIRE THAT FEDERAL, STATE, OR LOCAL AGENCIES INFORM INDIVIDUALS WHOSE SOCIAL SECURITY IS REQUESTED WHETHER SUCH DISCLOSURE IS MANDATORY OR VOLUNTARY, BASIS OF AUTHORITY FOR SUCH SOLICITATION, AND USES WHICH WILL BE MADE OF IT.</small>				
JUVENILE FINGERPRINT SUBMISSION YES <input type="checkbox"/> TREAT AS ADULT YES <input type="checkbox"/> [2.087]		DATE OF ARREST MM YY DD [2.045]		ORI CONTRIBUTOR [2.073] ADDRESS REPLY DESIRED? YES <input type="checkbox"/> TCN:[1.09] <i>[1.04]: CAR=Checked/CNA=Not Checked</i>
SEND COPY TO: (ENTER ONE) [2.007 #1] [2.007 #2]		DATE OF OFFENSE MM YY DD [2.047.1 #1]		PLACE OF BIRTH (STATE OR COUNTRY) [2.020] COUNTRY OF CITIZENSHIP [2.021]
MISCELLANEOUS NUMBERS [2.017 #1] [2.017 #2] [2.017 #3] [2.017 #4]		SCARS, MARKS, TATTOOS, AND AMPUTATIONS [2.026#1] [2.921.2 #1] [2.026#2] [2.921.2 #2]		
		RESIDENCE / COMPLETE ADDRESS [2.041]		CITY STATE
OFFICIAL TAKING FINGERPRINTS (NAME OR NUMBER) [2.480.1]		LOCAL IDENTIFICATION / REFERENCE LAN:[2.934] OCA:[2.009]		PHOTO AVAILABLE YES [2.036] PALM PRINTS TAKEN YES [2.035]
EMPLOYER: IF U.S. GOVERNMENT, INDICATE SPECIFIC AGENCY [2.039] IF MILITARY, LIST BRANCH OF SERVICE AND SERIAL NO.				OCCUPATION [2.040]
CHARGE / CITATION 1. [2.936.9 #1][2.047.2 #1] CNTS:[2.936.8#1] [2.936.7 #1][2.936.6 #1][2.936.5 #1]				DISPOSITION 1.[2.051 #1]
2. [2.936.9 #2][2.047.2 #2]CNTS:[2.936.8#2] [2.936.7 #2][2.936.6 #2] [2.936.5 #2]				2.[2.051 #2]
3. [2.936.9 #3][2.047.2 #3]CNTS:[2.936.8#3] [2.936.7 #3][2.936.6 #3] [2.936.5 #3]				3.[2.051 #3]
ADDITIONAL (if counts >4 NOTE: "nnn additional counts available") [2.936.9 #4][2.047.2 #4] CNTS:[2.936.8#4] [2.936.7 #4][2.936.6 #4] [2.936.5 #4]				[2.051 #4]
ADDITIONAL INFORMATION / BASIS FOR CAUTION [2.941.10][2.941.8][2.941.7] [2.941.9] [2.924.3][2.924.2][2.924.1] [2.088]				STATE BUREAU STAMP Central Sites: PRINT OUT SITE SPECIFIC ADDRESS
<small>FD-249 (REV. 12-1-84)</small>				<small>* U.S. GPO: 1987 432-177#0018</small>

5.5.3 Text and image placement on Federal Applicant fingerprint (FD-258) card (8 inches x 8 inches pre-printed), front (images) side only:

SID: [2.015 #1]		LEAVE BLANK		TYPE OR PRINT ALL INFORMATION IN BLACK				FBI LEAVE BLANK	
APPLICANT		LAST NAME NAM [2.018]		FIRST NAME [2.908.1#1] [2.908.2#1] [2.908.3#1] [2.908.4#1]		MIDDLE NAME			
SIGNATURE OF PERSON FINGERPRINTED		ALIAS AKA [2.019 #1]		O R I [2.073]				DATE OF BIRTH DOB [2.022]	
RESIDENCE OF PERSON FINGERPRINTED [2.041]		CITIZENSHIP CTZ [2.021]		SEX [2.024]	RACE [2.025]	HT [2.027]	WGT [2.029]	EYES [2.031]	HAIR [2.032]
DATE [2.038]	OFFICIAL TAKING FINGERPRINTS [2.480.1] [2.480.3]		YOUR NC. OCA [2.009]		PLACE OF BIRTH POB [2.020]				
EMPLOYER AND ADDRESS [2.039]		FBI NO. FBI [2.014]		TCN: [1.09] LEAVE BLANK CLASS _____ REF _____					
REASON FINGERPRINTED [2.037]		ARMED FORCES NO. MNU							
		SOCIAL SECURITY NO. [2.016]							
		MISCELLANEOUS NO. MNU [2.017#1]							
[2.084]/[2.124.2] #1		[2.084]/[2.124.2] #2		[2.084]/[2.124.2] #3		[2.084]/[2.124.2] #4		[2.084]/[2.124.2] #5	
[H.RT]		[H.RI]		[H.RM]		[H.RR]		[H.RL]	
1. R. THUMB		2. R. INDEX		3. R. MIDDLE		4. R. RING		5. R. LITTLE	
[2.084]/[2.124.2] #6		[2.084]/[2.124.2] #7		[2.084]/[2.124.2] #8		[2.084]/[2.124.2] #9		[2.084]/[2.124.2] #10	
[H.LT]		[H.LI]		[H.LM]		[H.LR]		[H.LL]	
6. L. THUMB		7. L. INDEX		8. L. MIDDLE		9. L. RING		10. L. LITTLE	
[2.067.1]	[2.067.2]	[2.067.3]	[2.038]	[PALETTE TARGETS]		[CURRENT PRINTER S/N]		[Current DATE:TIME]	
Scanner ID	Scanner S/N	[2.481]	[2.481]	(actual printer, not stored)		(actual Printer, not stored)		CCYYMMDDHHMM	
[H.L4]				[H.LTP]	[H.RTP]	[H.R4]			
LEFT FOUR FINGERS TAKEN SIMULTANEOUSLY				L THUMB	R THUMB	RIGHT FOUR FINGERS TAKEN SIMULTANEOUSLY			

5.5.4 Text and Image Placement on NEC Verification Form (8.5 inches x 11 inches Template Printed) - Front Side Only

TRANSACTION TYPE: [1.04]
 SID : [2.015]
 TCN : [1.09]
 Name: [2.018]
 -----AAAAAAAAAAAAAAAAAAAAAAAAAAAA
 Last : [2.908.1 #1]
 First : [2.908.2 #1]
 Middle: [2.908.3 #1]
 Suffix: [2.908.4 #1]
 Date of Birth: [2.022] SOC: [2.016] DLN: [2.910.1#1]
 [2.910.2#1]

-----NN/NN/NNNN-----NNNN-NN-NN-----AAAAAAAAAAAAAAAAAAAA
 Sex: [2.024] Race: [2.025] Height: [2.027] Weight: [2.029]
 -----A-----A-----NNN-----NNN
 Eye Color: [2.031] Hair Color: [2.032] MNU: [2.017#1]
 -----AAA-----AAA-----AAAAAAAAAAAAAAAAAAAA

[2.084/2.124.2]#1 [2.084/2.124.2]#2 [2.084/2.124.2]#3 [2.084/2.124.2]#4 [2.084/2.124.2]#5

 [H.RT] [H.RI] [H.RM] [H.RR] [H.RL]

[2.084/2.124.2]#6 [2.084/2.124.2]#7 [2.084/2.124.2]#8 [2.084/2.124.2]#9 [2.084/2.124.2]#10

 [H.LT] [H.LI] [H.LM] [H.LR] [H.LL]

[2.067.1] [2.067.2] [2.067.3] [2.038] PRINTER PALLETTE Printer Current
 [2.481] TARGETS S/N DATE

[H.L4] [H.LTP] [H.RTP] [H.R4]

TRANSACTION CONTROL NUMBER: [1.09]
 CONTROLLING AGENCY IDENTIFIER: [2.073 #1]
 ORIGINATING AGENCY IDENTIFIER: [1.08]
 ORIGINATING CASE IDENTIFIER: [2.009]
 DESTINATION AGENCY IDENTIFIER: [1.07]
 REASON FOR FINGERPRINTING: [2.037]
 INPUT FORM NAME: [IDX_IFMFL]
 INPUT FORM DESCRIPTION: [IDX_IFM]
 ALL Remaining Fields in Numerical Tag order number line break on each remaining field
 Ie [2.007] = "2.007 ""[2.007]
 Ie [2.008] = "2.008 ""[2.008]

Notes:

Explanatory Note (see below)

[1.XX]	Type 1 tag field reference
[2.XXX]	Type 2 tag XXX field reference
[2.XXX.Y]	Type 2 tag XXX subfield Y reference
[2.XXX.X #n]	Type 2 tag XXX subfield Y reference for instance number n
[H.AA]	High resolution image file for particular fingerprint's image: .RT = Rolled Right Thumb .RI = Rolled Right Index .RM = Rolled Right Middle .RR = Rolled Right Ring .RL = Rolled Right Little .LT = Rolled Left Thumb .LI = Rolled Left Index .LM = Rolled Left Middle .LR = Rolled Left Ring .LL = Rolled Left Little .RTP = Plain Right Thumb .LTP = Plain Left Thumb .L4 = Left Four Finger Simultaneous (plain) .R4 = Right Four Finger Simultaneous (plain)
[IDX_AAAA]	System generated field value.

Annotation (Tag: 2.084)

This applies to FD-249 pre-printed and template printed, FD-258 pre-printed and template printed and Transaction/Verification form printing.

If an Annotation B exists it will be displayed. If an Annotation A exists it will be displayed. If both exist, Annotation A will be displayed. If an Annotation B exists it will be printed in the upper left hand corner of the associated rolled fingerprint image box. If an Annotation A exists it will be printed in the upper left hand corner of the associated rolled fingerprint image box. If both A and B exist, A will be printed above B in the upper left hand corner of the associated rolled fingerprint image box.

5.5.5 WIN Standard Template – Palm Print

5.5.5.1 Text and image placement on WIN specific palm print form (8.5 inch x 11 inch page), front (images) side only – left palm:

<p>WIN PALM PRINT LEFT</p>	<p>UPPER PALM</p>
<p>ORI: [2.073] #1 NAME: [2.018] DOB: [2.022] #1 EM=(MM/DD/CCYY) SID: [2.015] FBI: [2.014] #1 DATE: [2.038] EM=(MM/DD/CCYY) TCN: [1.009] ATN: [2.006]</p> <p>OTP: [2.480.1] [Signature Image] OID: [2.480.2] – [2.480.3]</p>	<p>[H.LUP]</p>
<p>WRITER'S PALM</p> <p>[H.LWP]</p> <p>Scanner ID: [2.480.1] [2.480.2] Scanner S/N: [2.480.3] Printer: Current Printer S/N (Not in record) Current Date & Time EM=(MM/DD/CCYY HH:MM:SS) [PALETTE TARGETS]</p>	<p>[H.LP]</p> <p>[H.LLP]</p> <p>LOWER PALM</p>

5.5.5.2 Text and image placement on WIN specific palm print form (8.5 inch x 11 inch page), front (images) side only – right palm:

<p>WIN PALM PRINT RIGHT</p>	<p>UPPER PALM</p>
<p>ORI: [2.073] #1 NAME: [2.018] DOB: [2.022] #1 EM=(MM/DD/CCYY) SID: [2.015] FBI: [2.014] #1 DATE: [2.038] EM=(MM/DD/CCYY) TCN: [1.009] ATN: [2.006]</p> <p>OTP: [2.480.1] [Signature Image] OID: [2.480.2] – [2.480.3]</p>	<p>[H.RUP]</p>
<p>WRITER'S PALM</p> <p>[H.RWP]</p> <p>Scanner ID: [2.480.1] [2.480.2] Scanner S/N: [2.480.3] Printer: Current Printer S/N (Not in record) Current Date & Time EM=(MM/DD/CCYY HH:MM:SS) [PALETTE TARGETS]</p>	<p>[H.RP]</p> <p>[H.RLP]</p> <p>LOWER PALM</p>

5.6 Attachment F – WIN Member State Fingerprint Card Specifications

5.6.1 Alaska Fingerprint Card Print Specification

5.6.1.1 Text placement on Federal Criminal fingerprint (FD-249) card (8 inches x 8 inches pre-printed), front side:

LEAVE BLANK		CRIMINAL		(STAPLE HERE)					LEAVE BLANK								
				<input type="checkbox"/> NFF SECOND SUBMISSION <input type="checkbox"/> APPROXIMATE CLASS <input type="checkbox"/> AMPUTATION <input type="checkbox"/> SCAR													
STATE USAGE OCA: [2.009]				LAST NAME, FIRST NAME, MIDDLE NAME, SUFFIX [2.908.1][2.908.2" "[2.908.3" "[2.908.4" "] #1													
SIGNATURE OF PERSON FINGERPRINTED				SOCIAL SECURITY NO. [2.016 #1] [2.016 #2]				LEAVE BLANK TCN:[1.09]									
ALIASES/MAIDEN LAST NAME, FIRST NAME, MIDDLE NAME, SUFFIX [2.908.1][2.908.2" "[2.908.3" "[2.908.4" "] #2 [2.908.1][2.908.2" "[2.908.3" "[2.908.4" "] #3 [2.908.1][2.908.2" "[2.908.3" "[2.908.4" "] #4																	
FBI NO. [2.014#1]		STATE IDENTIFICATION NO. [2.015]		DATE OF BIRTH MM DD YY [2.022#1]		SEX [2.024]	RACE [2.025]	HEIGHT [2.913#1]	WEIGHT [2.914#1]	EYES [2.915#1]	HAIR [2.916#1]						
[2.124.2] #1 [2.124.3]#1		[2.124.2] #2 [2.124.3]#2		[2.124.2] #3 [2.124.3]#3		[2.124.2] #4 [2.124.3]#4		[2.124.2] #5 [2.124.3]#5									
[H.RT]		[H.RI]		[H.RM]		[H.RR]		[H.RL]									
[2.592.2] #1 [2.592.3]#1		[2.592.2] #2 [2.592.3]#2		[2.592.2] #3 [2.592.3]#3		[2.592.2] #4 [2.592.3]#4		[2.592.2] #5 [2.592.3]#5									
[2.124.2] #6 [2.124.3]#6		[2.124.2] #7 [2.124.3]#7		[2.124.2] #8 [2.124.3]#8		[2.124.2] #9 [2.124.3]#9		[2.124.2] #10 [2.124.3]#10									
[H.LT]		[H.LI]		[H.LM]		[H.LR]		[H.LL]									
[2.592.2] #6 [2.592.3]#6		[2.592.2] #7 [2.592.3]#7		[2.592.2] #8 [2.592.3]#8		[2.592.2] #9 [2.592.3]#9		[2.592.2] #10 [2.592.3]#10									
[2.067.1][2.067.2]		[2.067.3]		[2.038]		[PALETTE TARGETS]		[Current PRINTER S/N]		[Current DATE:TIME]							
SCANNER ID		SCANNER S/N		[2.481]		(actual printer, not stored)		(Actual Printer, Not Stored)									
[H.L4]				[H.LTP]		[H.RTP]		[H.R4]									
LEFT FOUR FINGERS TAKEN SIMULTANEOUSLY				L THUMB		R THUMB		RIGHT FOUR FINGERS TAKEN SIMULTANEOUSLY									

5.6.2 Alaska Fingerprint Card Print Specification

5.6.2.1 Text placement on Federal Criminal fingerprint (FD-249) card (8 inches x 8 inches pre-printed), rear side:

FEDERAL BUREAU OF INVESTIGATION, UNITED STATES DEPARTMENT OF JUSTICE WASHINGTON, D.C. 20537			
<small>PRIVACY ACT OF 1974 (P. L. 93-502) REQUIRES THAT FEDERAL, STATE, OR LOCAL AGENCIES INFORM INDIVIDUALS WHOSE SOCIAL SECURITY IS REQUESTED WHETHER SUCH DISCLOSURE IS MANDATORY OR VOLUNTARY, BASIS OF AUTHORITY FOR SUCH SOLICITATION, AND USES WHICH WILL BE MADE OF IT.</small>			
JUVENILE FINGERPRINT SUBMISSION [2.935.8] <input checked="" type="checkbox"/> YES <input type="checkbox"/> NO TREAT AS ADULT [2.935.8] YES <input type="checkbox"/> NO <input type="checkbox"/>		DATE OF ARREST [2.935.7] MM DD YY ORI [2.935.1] CONTRIBUTOR [2.935.2] ADDRESS [2.935.7] REPLY DESIRED? YES <input type="checkbox"/> NO <input type="checkbox"/> TCN: [1.009]	
SEND COPY TO: (ENTER ORI) [2.007 #1] [2.007 #2]		DATE OF OFFENSE [2.936.3 #1] MM DD YY PLACE OF BIRTH (STATE OR COUNTRY) [2.020] COUNTRY OF CITIZENSHIP [2.021]	
MISCELLANEOUS NUMBERS [2.909.1 #1]-[2.909.2#1] [2.909.1 #2]-[2.909.2#2] [2.909.1 #3]-[2.909.2#3] [2.909.1 #4]-[2.909.2#4]		SCARS, MARKS, TATTOOS, AND AMPUTATIONS [2.026#1] [2.026#2][2.026#3][2.026#4] [2.026#5] [2.026#6] [2.026#7][2.026#8][2.026#9] [2.026#10]	
OFFICIAL TAKING FINGERPRINTS (NAME OR NUMBER) [2.480.1] [2.480.2]- [2.480.3]		LOCAL IDENTIFICATION / REFERENCE [2.909.1 #1]:[2.909.2#1] OLN:[2.910.1#1]-[2.910.2#1] OLN:[2.910.1#2]-[2.910.2#2]	
EMPLOYER: IF U.S. GOVERNMENT, INDICATE SPECIFIC AGENCY IF MILITARY, LIST BRANCH OF SERVICE AND SERIAL NO. [2.922.2#1]		OCCUPATION [2.922.1]	
CHARGE / CITATION 1. [2.936.1 #1] [2.936.5 #1] CNTS:[2.936.8 #1] [2.936.9#1][2.936.2#1] [2.936.4 #1] [2.936.10 #1] [2.936.1 #2] [2.936.5 #2] CNTS:[2.936.8 #2] [2.936.9#2][2.936.2#2] [2.936.4 #2] [2.936.10 #2]		DISPOSITION 1.	
2. [2.936.1 #3][2.936.5 #3] CNTS:[2.936.8 #3] [2.936.9#3][2.936.2#3] [2.936.4 #3] [2.936.10 #3] [2.936.1 #4][2.936.5 #4] CNTS:[2.936.8 #4] [2.936.9#4][2.936.2#4] [2.936.4 #4] [2.936.10 #4]		2.	
3. [2.936.1 #5][2.936.5 #5] CNTS:[2.936.8 #5] [2.936.9#5][2.936.2#5] [2.936.4 #5] [2.936.10 #5] [2.936.1 #6][2.936.5 #6] CNTS:[2.936.8 #6] [2.936.9#6][2.936.2#6] [2.936.4 #6] [2.936.10 #6]		3.	
If counts > 6 Note: nnnadditional charges available"			
ADDITIONAL INFORMATION / BASIS FOR CAUTION [2.924.1 #1]		STATE BUREAU STAMP Received AK Dept. Of Public Safety @ current date & time	
<small>FD-249 (REV. 12-1-94)</small>		<small>* U.S. GPO: 1997 432-177/60018</small>	

5.6.3 Alaska Fingerprint Card Print Specification

5.6.3.1 Text and image placement on Federal Applicant fingerprint (FD-258) card (8 inches x 8 inches pre-printed), front (images) side only:

APPLICANT		LEAVE BLANK		TYPE OR PRINT ALL INFORMATION IN BLACK						FBI LEAVE BLANK	
SIGNATURE OF PERSON FINGERPRINTED		[2.908.1#1]		[2.908.2#1]		[2.908.3#1]		[2.908.4#1]			
RESIDENCE OF PERSON FINGERPRINTED [2.923.1]		[2.908.1 #2]		[2.908.1 #3]		[2.908.1 #4]		[2.908.1 #5]		DATE OF BIRTH DOB MONTH DAY YEAR [2.022]	
DATE [2.038]		SIGNATURE OF OFFICIAL TAKING FINGERPRINTS [2.480.1] [2.480.2]-[2.480.3]		CITIZENSHIP CTZ [2.021]		SEX [2.024]		RACE [2.025]		HGT [2.913]	
EMPLOYER AND ADDRESS [2.922.2#1]		YOUR NO. OCA [2.009]		FBI NO. FBI [2.014]		WGT [2.914]		EYES [2.915]		HAIR [2.916]	
REASON FINGERPRINTED [2.037]		ARMED FORCES NO. MNU [2.909.1#1]-[2.909.2#1]		SOCIAL SECURITY NO. [2.016#1]		MISCELLANEOUS NO. MNU [2.015]		CLIENT ID: [2.479.2] LEAVE BLANK		Lic.Agy: [2.479.7]	
								TCN: [1.09]		PLACE OF BIRTH POB [2.020]	
								CLASS _____		REF _____	
								DL: [2.910.1#1] [2.910.2#1]			
[2.124.2] #1 [2.124.3] #1		[2.124.2] #2 [2.124.3] #2		[2.124.2] #3 [2.124.3] #3		[2.124.2] #4 [2.124.3] #4		[2.124.2] #5 [2.124.3] #5			
[H.RT]		[H.RI]		[H.RM]		[H.RR]		[H.RL]			
[2.592.2] #1 [2.592.3] #1		[2.592.2] #2 [2.592.3] #2		[2.592.2] #3 [2.592.3] #3		[2.592.2] #4 [2.592.3] #4		[2.592.2] #5 [2.592.3] #5			
[2.124.2] #6 [2.124.3] #6		[2.124.2] #7 [2.124.3] #7		[2.124.2] #8 [2.124.3] #8		[2.124.2] #9 [2.124.3] #9		[2.124.2] #10 [2.124.3] #10			
[H.LT]		[H.LI]		[H.LM]		[H.LR]		[H.LL]			
[2.592.2] #6 [2.592.3] #6		[2.592.2] #7 [2.592.3] #7		[2.592.2] #8 [2.592.3] #8		[2.592.2] #9 [2.592.3] #9		[2.592.2] #10 [2.592.3] #10			
[2.067.1] [2.067.2] [2.067.3]		[2.038]		[PALETTE TARGETS]		[CURRENT PRINTER S/N]		[Current DATE:TIME]			
Scanner ID		Scanner S/N		[2.481]		(actual printer, not stored)		(actual Printer, not stored)		ccYYMMDD:HH:MM	
[H.L4]		[H.LTP]		[H.RTP]		[H.R4]					
LEFT FOUR FINGERS TAKEN SIMULTANEOUSLY		L. THUMB		R. THUMB		RIGHT FOUR FINGERS TAKEN SIMULTANEOUSLY					

Alaska Template Notes:

1. All dates are formatted for printing as MM/DD/CCYY
2. If 2.919.1 has a value it is printed on the left and the check box is checked.
3. If 2.918.1 has a value it is printed on the left and the check box is checked.
4. If the value of 2.935.8 is "Juvenile" then the "submission" check box should be checked. If the value is "Juvenile as Adult" then both the "submission" and the "treat as adult" check boxes should be checked.

5.6.4.2 Text and image placement on WIN specific palm print form (8.5 inch x 11 inch page), front (images) side only – right palm:

<p>ALASKA PALM PRINT RIGHT</p>	<p>UPPER PALM</p>
<p>ORI: [2.935.1] NAME: [2.908.1], [2.908.2] [2.908.3] [2.908.4] #1 DOB: [2.022] #1 EM=(MM/DD/CCYY) SID: [2.015] FBI: [2.014] #1 DATE: [2.038] EM=(MM/DD/CCYY) TCN: [1.009] ATN: [2.599.2] #1</p> <p>OTP: [2.480.1] Signature Image OID: [2.480.2] – [2.480.3]</p>	<p>[H.RUP]</p>
<p>WRITER'S PALM</p> <p>[H.RWP]</p> <p>Scanner ID: [2.480.1] [2.480.2] Scanner S/N: [2.480.3] Printer: Current Printer S/N (Not in record) Current Date & Time EM=(MM/DD/CCYY HH:MM:SS) [PALETTE TARGETS]</p>	<p>LOWER PALM</p> <p>[H.RLP]</p>

5.6.5 Idaho Specific Template - Applicant

5.6.5.1 Text and image placement on Federal Applicant fingerprint (FD-258) card (8 inches x 8 inches pre-printed), front (images) side only:

APPLICANT		LEAVE BLANK SID: [2.015 #1] TCN: [1.09]		TYPE OR PRINT ALL INFORMATION IN BLACK						FBI LEAVE BLANK		
SIGNATURE OF PERSON FINGERPRINTED		LAST NAME NAM [2.018]		FIRST NAME [2.908.1#1]		MIDDLE NAME [2.908.2#1]		[2.908.3#1]		[2.908.4#1]		
RESIDENCE OF PERSON FINGERPRINTED [2.041]		ALIAS AKA [2.019 #1]		OR I		[2.073]		DATE OF BIRTH DOB MONTH DAY YEAR [2.022]				
DATE [2.038]		SIGNATURE OF OFFICIAL TAKING FINGERPRINTS [2.480.1] [2.480.2] [2.480.3]		CITIZENSHIP CTZ [2.021]		SEX [2.024]	RACE [2.025]	HGT [2.027]	WGT [2.029]	EYES [2.031]	HAIR [2.032]	PLACE OF BIRTH POB [2.020]
EMPLOYER AND ADDRESS [2.039]		YOUR NO. OCA [2.009]		LEAVE BLANK								
REASON FINGERPRINTED [2.037]		FBI NO. FBI [2.014]										
		ARMED FORCES NO. MNU										
		SOCIAL SECURITY NO. [2.016]										
		MISCELLANEOUS NO. MNU [2.017#1]		CLASS _____		REF _____						
[2.084]/[2.124.2] #1		[2.084]/[2.124.2] #2		[2.084]/[2.124.2] #3		[2.084]/[2.124.2] #4		[2.084]/[2.124.2] #5				
[H.RT]		[H.RI]		[H.RM]		[H.RR]		[H.RL]				
1. R. THUMB		2. R. INDEX		3. R. MIDDLE		4. R. RING		5. R. LITTLE				
[2.084]/[2.124.2] #6		[2.084]/[2.124.2] #7		[2.084]/[2.124.2] #8		[2.084]/[2.124.2] #9		[2.084]/[2.124.2] #10				
[H.LT]		[H.LI]		[H.LM]		[H.LR]		[H.LL]				
6. L. THUMB		7. L. INDEX		8. L. MIDDLE		9. L. RING		10. L. LITTLE				
[2.067.1] [2.067.2] [2.067.3] Scanner ID Scanner S/N		[2.038] [2.481] [2.481]		[PALETTE TARGETS] (actual printer, not stored)		[CURRENT PRINTER S/N] (actual Printer, not stored)		[Current DATE:TIME] CCYYMMDD:HH:MM				
				[H.LTP] [H.RTP]		[H.R4]						
				L. THUMB		R. THUMB		RIGHT FOUR FINGERS TAKEN SIMULTANEOUSLY				

5.6.6 Idaho Specific Template – Corrections Card - Front

5.6.6.1 Text placement on Federal Criminal fingerprint (FD-249) card (8 inches x 8 inches pre-printed), front side:

LEAVE BLANK CRIMINAL SID:[2.015 #1]		(STAPLE HERE) <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <small>NFF SECOND SUBMISSION APPROXIMATE CLASS AMPUTATION SCAR</small>			LEAVE BLANK				
STATE USAGE CASE-NUM: [2.934] TCN:[1.09]		LAST NAME, FIRST NAME, MIDDLE NAME, SUFFIX [2.018] [2.908.1][2.908.2" "[2.908.3" "[2.908.4" "] #1							
SIGNATURE OF PERSON FINGERPRINTED		SOCIAL SECURITY NO. [2.016 #1] [2.016 #2]		LEAVE BLANK					
ALIASES/MAIDEN LAST NAME, FIRST NAME, MIDDLE NAME, SUFFIX [2.019 #1] [2.908.1][2.908.2" "[2.908.3" "[2.908.4" "] #2 [2.019 #2] [2.908.1][2.908.2" "[2.908.3" "[2.908.4" "] #3									
FBI NO. [2.014#1]	STATE IDENTIFICATION NO. [2.015#1]	DATE OF BIRTH MM DD YY [2.022#1]	SEX [2.024]	RACE [2.025]	HEIGHT [2.027]	WEIGHT [2.029]	EYES [2.031]	HAIR [2.032]	
[2.084]/[2.124.2] #1 [H.RT] <small>1. R. THUMB</small>	[2.084]/[2.124.2] #2 [H.RI] <small>2. R. INDEX</small>	[2.084]/[2.124.2] #3 [H.RM] <small>3. R. MIDDLE</small>	[2.084]/[2.124.2] #4 [H.RR] <small>4. R. RING</small>	[2.084]/[2.124.2] #5 [H.RL] <small>5. R. LITTLE</small>					
[2.084]/[2.124.2] #6 [H.LT] <small>6. L. THUMB</small>	[2.084]/[2.124.2] #7 [H.LI] <small>7. L. INDEX</small>	[2.084]/[2.124.2] #8 [H.LM] <small>8. L. MIDDLE</small>	[2.084]/[2.124.2] #9 [H.LR] <small>9. L. RING</small>	[2.084]/[2.124.2] #10 [H.LL] <small>10. L. LITTLE</small>					
[2.067.1][2.067.2] SCANNER ID	[2.067.3] SCANNER S/N	[2.038] [2.481]			[Current PRINTER S/N] (Actual Printer, Not Stored)		[Current DATE:TIME]		
[H.L4] <small>LEFT FOUR FINGERS TAKEN SIMULTANEOUSLY</small>			[H.LTP] <small>L. THUMB</small>	[H.RTP] <small>R. THUMB</small>	[H.R4] <small>RIGHT FOUR FINGERS TAKEN SIMULTANEOUSLY</small>				

5.6.7 Idaho Specific Template – Corrections Card - Rear

5.6.7.1 Text placement on Federal Criminal fingerprint (FD-249) card (8 inches x 8 inches pre-printed), rear side:

FEDERAL BUREAU OF INVESTIGATION, UNITED STATES DEPARTMENT OF JUSTICE WASHINGTON, D.C. 20537				SID: [2.015 #1]
<small>PRIVACY ACT OF 1974 (P.L. 93-579) REQUIRES THAT FEDERAL, STATE, OR LOCAL AGENCIES INFORM INDIVIDUALS WHOSE SOCIAL SECURITY IS REQUESTED WHETHER SUCH DISCLOSURE IS MANDATORY OR VOLUNTARY, BASIS OF AUTHORITY FOR SUCH SOLICITATION, AND USES WHICH WILL BE MADE OF IT.</small>				
JUVENILE FINGERPRINT SUBMISSION YES <input type="checkbox"/> TREAT AS ADULT YES <input type="checkbox"/> [2.087]		DATE OF ARREST MM DD YY [2.045]		ORI CONTRIBUTOR [2.073] ADDRESS REPLY DESIRED? YES <input type="checkbox"/> TCN:[1.09] <i>[1.04]: CAR=Checked/CNA=Not Checked</i>
SEND COPY TO: #ENTER Q81 [2.007 #1] [2.007 #2]		DATE OF OFFENSE MM DD YY [2.047.1 #1]		PLACE OF BIRTH (STATE OR COUNTRY) [2.020]
MISCELLANEOUS NUMBERS [2.017 #1] [2.017 #2] [2.017 #3] [2.017 #4]		SCARS, MARKS, TATTOOS, AND AMPUTATIONS [2.026#1] [2.921.2 #1] [2.026#2] [2.921.2 #2]		
		RESIDENCE / COMPLETE ADDRESS [2.041]		CITY STATE
OFFICIAL TAKING FINGERPRINTS (NAME OR NUMBER) [2.480.1]		LOCAL IDENTIFICATION /REFERENCE LAN:[2.934] OCA:[2.009]		PHOTO AVAILABLE YES <input type="checkbox"/> [2.036] PALM PRINTS TAKEN YES <input type="checkbox"/> [2.035]
EMPLOYER: IF U.S. GOVERNMENT, INDICATE SPECIFIC AGENCY IF MILITARY, LIST BRANCH OF SERVICE AND SERIAL NO. [2.039]		OCCUPATION [2.040]		
CHARGE / CITATION 1. [2.938.12#1] [2.938.15#1] [2.938.13#1] [2.938.1#1] [2.938.10#1]		DISPOSITION 1. [2.051.1]		
2. [2.938.12#2] [2.938.15#2] [2.938.13#2] [2.938.1#2] [2.938.10#2]		2. [2.051.2]		
3. [2.938.12#3] [2.938.15#3] [2.938.13#3] [2.938.1#3] [2.938.10#3]		3. [2.051.3]		
ADDITIONAL [if counts >4 NOTE: "nnn additional counts available"] [2.938.12#4] [2.938.15#4] [2.938.13#4] [2.938.1#4] [2.938.10#4]		[2.051.4]		
ADDITIONAL INFORMATION /BASIS FOR CAUTION [2.941.10][2.941.8][2.941.7] [2.941.9] [2.924.3][2.924.2][2.924.1] [2.088]		STATE BUREAU STAMP Central Sites: PRINT OUT SITE SPECIFIC ADDRESS		
<small>FD-249 (REV. 12-1-64)</small>		<small>*U.S. GPO: 1997 432-17760018</small>		

5.6.8 Oregon Specific Template – Criminal

5.6.8.1 Text placement on Federal Criminal fingerprint (FD-249) card (8 inches x 8 inches pre-printed), front side:

LEAVE BLANK		CRIMINAL		(STAPLE HERE)					LEAVE BLANK	
		<input type="checkbox"/> NFF SECOND SUBMISSION <input type="checkbox"/> APPROXIMATE CLASS <input type="checkbox"/> AMPUTATION <input type="checkbox"/> SCAR								
STATE USAGE [1.09 w/out 'OR']		LAST NAME, FIRST NAME, MIDDLE NAME, SUFFIX [2.908.1 #1],[2.908.2 #1] [2.908.3 #1] [2.908.4 #1]								
SIGNATURE OF PERSON FINGERPRINTED		SOCIAL SECURITY NO. [2.016 #1] [2.016 #2]		LEAVE BLANK						
ALIASES/MAIDEN LAST NAME, FIRST NAME, MIDDLE NAME, SUFFIX [2.908.1 #2],[2.908.2 #2] [2.908.3 #2] [2.908.4 #2] [2.908.1 #3],[2.908.2 #3] [2.908.3 #3] [2.908.4 #3] [2.908.1 #4],[2.908.2 #4] [2.908.3 #4] [2.908.4 #4] [2.908.1 #5],[2.908.2 #5] [2.908.3 #5] [2.908.4 #5]										
FBI NO. [2.014 #1]	STATE IDENTIFICATION NO. [2.015 #1]	DATE OF BIRTH MM DD YY [2.022 #1]		SEX [2.024]	RACE [2.025]	HEIGHT [2.027]	WEIGHT [2.029]	EYES [2.031]	HAIR [2.032]	
[H.RT]	[H.RI]	[H.RM]		[H.RR]		[H.RL]				
1. R. THUMB	2. R. INDEX	3. R. MIDDLE		4. R. RING		5. R. LITTLE				
[H.LT]	[H.LI]	[H.LM]		[H.LR]		[H.LL]				
6. L. THUMB	7. L. INDEX	8. L. MIDDLE		9. L. RING		10. L. LITTLE				
[2.067.3] [2.067.1] [2.067.2] [2.038] [2.481]		[PALETTE TARGETS] (actual printer, not stored)		Printer Model	Mnemonic	[Current DATE:TIME] CCYYMMDD:HH:MM:SS				
[H.L4]		[H.LTP]	[H.RTP]	[H.R4]						
LEFT FOUR FINGERS TAKEN SIMULTANEOUSLY										

5.6.8.2 Text placement on Federal Criminal fingerprint (FD-249) card (8 inches x 8 inches pre-printed), rear side:

FEDERAL BUREAU OF INVESTIGATION, UNITED STATES DEPARTMENT OF JUSTICE WASHINGTON, D.C. 20537			
<small>PRIVACY ACT (P.L. 93-502) REQUIRES THAT FEDERAL, STATE, OR LOCAL AGENCIES INFORM INDIVIDUALS WHOSE SOCIAL SECURITY IS REQUESTED WHETHER SUCH DISCLOSURE IS MANDATORY OR VOLUNTARY. BASIS OF AUTHORITY FOR SUCH SOLICITATION AND USES WHICH WILL BE MADE OF IT.</small>			
JUVENILE FINGERPRINT SUBMISSION YES <input type="checkbox"/> TREAT AS ADULT YES <input type="checkbox"/> [2.087]	DATE OF ARREST MM-DD-YY [2.045]	[2.073] [Contributing Agency Literal] [Contributing Agency Name] REPLY DESIRED? YES <input type="checkbox"/> TCN [1.09] [1.04]: CAR=Checked/CNA=Not Checked	
SEND COPY TO: (ENTER OR) [2.007 #1] [2.007 #2]	DATE OF OFFENSE MM-DD-YY [2.047.1 #1]	PLACE OF BIRTH (STATE OR COUNTRY) [2.020]	COUNTRY OF CITIZENSHIP [2.021]
MISCELLANEOUS NUMBERS [2.017 #1] [2.017 #2] [2.017 #3] [2.017 #4]	SCARS, MARKS, TATTOOS, AND AMPUTATIONS [2.026 #1] [2.026 #3] [2.026 #5] [2.026 #7] [2.026 #9] [2.026 #2] [2.026 #4] [2.026 #6] [2.026 #8] [2.026 #10]		
	RESIDENCE / COMPLETE ADDRESS [2.041]	CITY	STATE
OFFICIAL TAKING FINGERPRINTS (NAME OR NUMBER) [2.480.1] [2.480.2] [2.480.3]	LOCAL IDENTIFICATION / REFERENCE LAN: [2.934] OCA: [2.009]		PHOTO AVAILABLE YES <input type="checkbox"/> [2.036] PALM PRINTS TAKEN YES <input type="checkbox"/> [2.035] [2.918 #1]
EMPLOYER: IF U.S. GOVERNMENT, INDICATE SPECIFIC AGENCY IF MILITARY, LIST BRANCH OF SERVICE AND SERIAL NO. [2.039]		OCCUPATION [2.040]	
CHARGE / CITATION 1.1. [2.936.9 #1] [2.936.5 #1] [2.936.4 #1] CNTS: [2.936.8 #1] [2.936.10 #1] 2. [2.936.9 #2] [2.936.5 #2] [2.936.4 #2] CNTS: [2.936.8 #2] [2.936.10 #2] 3. [2.936.9 #3] [2.936.5 #3] [2.936.4 #3] CNTS: [2.936.8 #3] [2.936.10 #3] 3. 4. [2.936.9 #4] [2.936.5 #4] [2.936.4 #4] CNTS: [2.936.8 #4] [2.936.10 #4] 5. [2.936.9 #5] [2.936.5 #5] [2.936.4 #5] CNTS: [2.936.8 #5] [2.936.10 #5]		DISPOSITION 1.1. [2.938.1 #1] [2.938.2 #1] [2.938.15 #1] [2.938.12 #1] [2.938.11 #1] 2. CNTS: [2.938.14 #1] [2.938.10 #1] [2.938.17 #1] [2.938.18 #1] [2.938.7 #1] [2.938.16 #1] [2.938.19 #1] 3. 2. [2.938.1 #2] [2.938.2 #2] [2.938.15 #2] [2.938.12 #2] [2.938.11 #2]	
ADDITIONAL 6. [2.936.9 #6] [2.936.5 #6] [2.936.4 #6] CNTS: [2.936.8 #6] [2.936.10 #6]		CNTS: [2.938.14 #2] [2.938.10 #2] [2.938.17 #2] [2.938.18 #2] [2.938.7 #2] [2.938.16 #2] [2.938.19 #2]	
ADDITIONAL INFORMATION / BASIS FOR CAUTION 7. [2.936.9 #7] [2.936.5 #7] [2.936.4 #7] CNTS: [2.936.8 #7] [2.936.10 #7] 8. [2.936.9 #8] [2.936.5 #8] [2.936.4 #8] CNTS: [2.936.8 #8] [2.936.10 #8]		STATE BUREAU STAMP Oregon State Police Identification Services Section 3772 Portland Rd NE Salem, Oregon 97301-2500	

FD-249 (REV. 12-1-94)

* U.S. GPO: 1997 432-177/60018

5.6.9 Oregon Specific Template – Applicant

5.6.9.1 Text and image placement on Federal Applicant fingerprint (FD-258) card (8 inches x 8 inches pre-printed), front (images) side only:

APPLICANT		LEAVE BLANK		TYPE OR PRINT ALL INFORMATION IN BLACK						FBI LEAVE BLANK	
		LAST NAME NAM		FIRST NAME		MIDDLE NAME					
		[2.908.1 #1],		[2.908.2 #1]		[2.908.3 #1]		[2.908.4 #1]			
SIGNATURE OF PERSON FINGERPRINTED		ALIAS AKA		O R I		[2.073]		[Contributing Agency Literal]		DATE OF BIRTH DOB	
[2.041]		[2.908.1 #2],		[2.908.2 #2]		[2.908.3 #2]		[2.908.4 #2]		MONTH DAY YEAR	
RESIDENCE OF PERSON FINGERPRINTED		[2.908.3 #2]		[2.908.4 #2]		[Contributing Agency Name]				[2.022]	
[2.041]		CITIZENSHIP CTZ		SEX		RACE		HT		WGT	
[2.038]		[2.021]		[2.024]		[2.025]		[2.027]		[2.029]	
DATE		SIGNATURE OF OFFICIAL TAKING FINGERPRINTS		YOUR NO. OCA		EYES		HAIR		PLACE OF BIRTH POB	
[2.038]		[2.480.1]		[2.009]		[2.031]		[2.032]		[2.020]	
[2.480.2]		[2.480.3]		FBI NO. FBI		LEAVE BLANK					
EMPLOYER AND ADDRESS		ARMED FORCES NO. MNU		SOCIAL SECURITY NO.		MISCELLANEOUS NO. MNU		TCN/ [1.09]			
[2.039]		[2.017 #1]		[2.016]		[2.017 #1]		CLASS _____			
REASON FINGERPRINTED								REF _____			
[2.037]											
[H.RT]		[H.RI]		[H.RM]		[H.RR]		[H.RL]			
1. R. THUMB		2. R. INDEX		3. R. MIDDLE		4. R. RING		5. R. LITTLE			
[H.LT]		[H.LI]		[H.LM]		[H.LR]		[H.LL]			
6. L. THUMB		7. L. INDEX		8. L. MIDDLE		9. L. RING		10. L. LITTLE			
[2.067.3] [2.067.1] [2.067.2] [2.038] [2.481]		[H.L4]		[PALETTE TARGETS] (actual printer, not stored)		[H.LTP] [H.RTP]		Printer Model Mnemonic		[Current DATE:TIME] CCYYMMDD:HH:MM:SS	
LEFT FOUR FINGERS TAKEN SIMULTANEOUSLY		L. THUMB		R. THUMB		RIGHT FOUR FINGERS TAKEN SIMULTANEOUSLY					

5.6.10 Oregon Specific Template – Palm Print

5.6.10.1 Text and image placement on WIN specific palm print form (8.5 inch x 11 inch page), front (images) side only – right palm:

SID: [2.015]	LAST NAME NAM [2.908.1 #1],	FIRST NAME [2.908.2 #1]	MIDDLE NAME [2.908.3 #1]	[2.908.4 #1]	SEX: [2.024]	RACE: [2.025]	DOB: [2.022]
DATE PRINTED [2.038]	TAKEN BY [2.480.1]	[2.480.2] [2.480.3]			ORI: [2.073]	OCA: [2.009]	
[2.067.3] [2.067.1] [2.067.2] [2.038] [2.481] RIGHT WRITER S PALM				Printer Model Mnemonic RIGHT UPPER/FULL PALM		[Current DATE:TIME] CCYYMMDD:HHMM	
[H.RW]				[H.RUP]			
				[H.RP]			
				[H.RLP]			
				RIGHT LOWER PALM			

5.6.11 Text and image placement on WIN specific palm print form (8.5 inch x 11 inch page), front (images) side only – left palm:

SID: [2.015]	LAST NAME NAM [2.908.1 #1],	FIRST NAME [2.908.2 #1]	MIDDLE NAME [2.908.3 #1]	[2.908.4 #1]	SEX: [2.024]	RACE: [2.025]	DOB: [2.022]
DATE PRINTED [2.038]	TAKEN BY [2.480.1] [2.480.2] [2.480.3]			ORI: [2.073]	OCA: [2.009]		
[2.067.3] [2.067.1] [2.067.2] [2.038] [2.481] LEFT WRITER'S PALM				Printer Model Mnemonic LEFT UPPERFULL PALM		[Contributing Agency Name]	
[H.LW]				[H.LUP]			
				[H.LP]			
				[H.LLP]			
LEFT LOWER PALM							

5.6.12 Utah Specific Template – Criminal

5.6.12.1 Text placement on Federal Criminal fingerprint (FD-249) card (8 inches x 8 inches pre-printed), front side:


LEAVE BLANK CRIMINAL SID:[2.015 #1] AORI: [2.935.1]		(STAPLE HERE) <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> NFF SECOND APPROXIMATE CLASS AMPUTATION SCAR SUBMISSION			LEAVE BLANK			
STATE USAGE CASE-NUM: [2.934] TCN:[1.09]		LAST NAME, FIRST NAME, MIDDLE NAME, SUFFIX [2.018] [2.908.1][2.908.2" "[2.908.3" "[2.908.4" "] #1						
SIGNATURE OF PERSON FINGERPRINTED		SOCIAL SECURITY NO. [2.016 #1] [2.016 #2]		LEAVE BLANK				
ALIASES/MAIDEN LAST NAME, FIRST NAME, MIDDLE NAME, SUFFIX [2.019 #1] [2.908.1][2.908.2" "[2.908.3" "[2.908.4" "] #2 [2.019 #2] [2.908.1][2.908.2" "[2.908.3" "[2.908.4" "] #3								
FBI NO. [2.014#1]	STATE IDENTIFICATION NO. [2.015#1]	DATE OF BIRTH MM DD YY [2.022#1]	SEX [2.024]	RACE [2.025]	HEIGHT [2.027]	WEIGHT [2.029]	EYES [2.031]	HAIR [2.032]
[2.084]/[2.124.2] #1 [H.RT] 1. R. THUMB	[2.084]/[2.124.2] #2 [H.RI] 2. R. INDEX	[2.084]/[2.124.2] #3 [H.RM] 3. R. MIDDLE	[2.084]/[2.124.2] #4 [H.RR] 4. R. RING	[2.084]/[2.124.2] #5 [H.RL] 5. R. LITTLE	[2.084]/[2.124.2] #10 [H.LL] 10. L. LITTLE			
[2.084]/[2.124.2] #6 [H.LT] 6. L. THUMB	[2.084]/[2.124.2] #7 [H.LI] 7. L. INDEX	[2.084]/[2.124.2] #8 [H.LM] 8. L. MIDDLE	[2.084]/[2.124.2] #9 [H.LR] 9. L. RING	[2.084]/[2.124.2] #10 [H.LL] 10. L. LITTLE				
[2.067.1][2.067.2] SCANNER ID		[2.067.3] SCANNER S/N	[2.038] [2.481]	[Current PRINTER S/N] (Actual Printer, Not Stored)		[Current DATE:TIME]		
[H.L4] LEFT FOUR FINGERS TAKEN SIMULTANEOUSLY		[H.LTP] L THUMB	[H.RTP] R THUMB	[H.R4] RIGHT FOUR FINGERS TAKEN SIMULTANEOUSLY				

5.6.12.2 Text placement on Federal Criminal fingerprint (FD-249) card (8 inches x 8 inches pre-printed), rear side:


FEDERAL BUREAU OF INVESTIGATION, UNITED STATES DEPARTMENT OF JUSTICE WASHINGTON, D.C. 20537				SID: [2.015 #1]
<small>PRIVACY ACT OF 1974 (P. L. 93-579) REQUIRES THAT FEDERAL, STATE, OR LOCAL AGENCIES INFORM INDIVIDUALS WHOSE SOCIAL SECURITY IS REQUESTED WHETHER SUCH DISCLOSURE IS MANDATORY OR VOLUNTARY, BASIS OF AUTHORITY FOR SUCH SOLICITATION, AND USES WHICH WILL BE MADE OF IT.</small>				
JUVENILE FINGERPRINT SUBMISSION YES <input type="checkbox"/>		DATE OF ARREST MM DD YY [2.045]		ORI CONTRIBUTOR [2.073] ADDRESS REPLY DESIRED? YES <input type="checkbox"/> TCN:[1.09] <i>[1.04]: CAR=Checked/CNA=Not Checked</i>
TREAT AS ADULT [2.087] YES <input type="checkbox"/>		SEND COPY TO: (ENTER ORI) [2.007 #1] [2.007 #2]		DATE OF OFFENSE MM DD YY [2.047.1 #1]
MISCELLANEOUS NUMBERS [2.017 #1] [2.017 #2] [2.017 #3] [2.017 #4]		PLACE OF BIRTH (STATE OR COUNTRY) [2.020]		COUNTRY OF CITIZENSHIP [2.021]
SCARS, MARKS, TATTOOS, AND AMPUTATIONS [2.026#1] [2.921.2 #1] [2.026#2] [2.921.2 #2]		RESIDENCE / COMPLETE ADDRESS [2.041]		CITY STATE
OFFICIAL TAKING FINGERPRINTS (NAME OR NUMBER) [2.480.1]		LOCAL IDENTIFICATION / REFERENCE LAN:[2.934] OCA:[2.009]		PHOTO AVAILABLE YES <input type="checkbox"/> [2.036] PALM PRINTS TAKEN YES <input type="checkbox"/> [2.035]
EMPLOYER: IF U.S. GOVERNMENT, INDICATE SPECIFIC AGENCY IF MILITARY, LIST BRANCH OF SERVICE AND SERIAL NO. [2.039]		OCCUPATION [2.040]		
CHARGE / CITATION 1. [2.936.6 #1][2.936.7 #1] [2.936.9#1] [2.936.4#1] [2.936.10#1]		DISPOSITION 1. [2.051 #1]		
2. [2.936.6 #2][2.936.7 #2] [2.936.9#2] [2.936.4#2] [2.936.10#2]		2. [2.051 #2]		
3. [2.936.6 #3][2.936.7 #3] [2.936.9#3] [2.936.4#3] [2.936.10#3]		3. [2.051 #3]		
ADDITIONAL [if counts >4 NOTE: "nnn additional counts available"] [2.936.6 #4][2.936.7 #4] [2.936.9#4] [2.936.4#4][2.936.10#4]		[2.051 #4]		
ADDITIONAL INFORMATION / BASIS FOR CAUTION [2.941.10][2.941.8][2.941.7] [2.941.9] [2.924.3][2.924.2][2.924.1] [2.088]		STATE BUREAU STAMP Central Sites: PRINT OUT SITE SPECIFIC ADDRESS		
<small>FD-249 (REV. 12-1-94)</small>		<small>* U.S. GPO: 1997 432-177/60018</small>		

5.6.13 Washington Specific Template – Criminal

5.6.13.1 Text placement on Federal Criminal fingerprint (FD-249) card (8 inches x 8 inches pre-printed), front side:


LEAVE BLANK CRIMINAL  TCN:[1.09]		(STAPLE HERE) <input type="checkbox"/> NFF SECOND SUBMISSION <input type="checkbox"/> APPROXIMATE CLASS <input type="checkbox"/> AMPUTATION <input type="checkbox"/> SCAR			LEAVE BLANK			
STATE USAGE		LAST NAME, FIRST NAME, MIDDLE NAME, SUFFIX [2.018]						
SIGNATURE OF PERSON FINGERPRINTED		SOCIAL SECURITY NO. [2.016]		LEAVE BLANK				
ALIASES/MAIDEN LAST NAME, FIRST NAME, MIDDLE NAME, SUFFIX [2.019] #1 [2.019] #2 [2.019] #3		[2.022] #1 (DOB Alias) [2.022] #2 (DOB Alias) [2.022] #3 (DOB Alias)						
FBI NO. [2.014]	STATE IDENTIFICATION NO. [2.015]	DATE OF BIRTH MM DD YY [2.022]	SEX [2.024]	RACE [2.025]	HEIGHT [2.027]	WEIGHT [2.029]	EYES [2.031]	HAIR [2.032]
[2.084] #1 (AMP/FGP/AMPCD) [H.RT] 1. R. THUMB	[2.084] #2 (AMP/FGP/AMPCD) [H.RI] 2. R. INDEX	[2.084] #3 (AMP/FGP/AMPCD) [H.RM] 3. R. MIDDLE	[2.084] #4 (AMP/FGP/AMPCD) [H.RR] 4. R. RING	[2.084] #5 (AMP/FGP/AMPCD) [H.RL] 5. R. LITTLE				
[2.084] #6 (AMP/FGP/AMPCD) [H.LT] 6. L. THUMB	[2.084] #7 (AMP/FGP/AMPCD) [H.LI] 7. L. INDEX	[2.084] #8 (AMP/FGP/AMPCD) [H.LM] 8. L. MIDDLE	[2.084] #9 (AMP/FGP/AMPCD) [H.LR] 9. L. RING	[2.084] #10 (AMP/FGP/AMPCD) [H.LL] 10. L. LITTLE				
[2.067.1][2.067.2] SCANNER ID [H.L4] LEFT FOUR FINGERS TAKEN SIMULTANEOUSLY		[2.067.3] [2.038] SCANNER S/N [2.481] [H.LTP] [H.RTP] L. THUMB R. THUMB		[Current PRINTER S/N] (Actual Printer, Not Stored)		[Current DATE:TIME]		
			[H.R4] RIGHT FOUR FINGERS TAKEN SIMULTANEOUSLY					

5.6.13.2 Text placement on Federal Criminal fingerprint (FD-249) card (8 inches x 8 inches pre-printed), rear side:

FEDERAL BUREAU OF INVESTIGATION, UNITED STATES DEPARTMENT OF JUSTICE WASHINGTON, D.C. 20537			
<small>PRIVACY ACT OF 1974 (P. L. 93-579) REQUIRES THAT FEDERAL, STATE, OR LOCAL AGENCIES INFORM INDIVIDUALS WHOSE SOCIAL SECURITY IS REQUESTED WHETHER SUCH DISCLOSURE IS MANDATORY OR VOLUNTARY, BASIS OF AUTHORITY FOR SUCH SOLICITATION, AND USES WHICH WILL BE MADE OF IT.</small>			
JUVENILE FINGERPRINT SUBMISSION YES <input type="checkbox"/> TREAT AS ADULT YES <input type="checkbox"/>		DATE OF ARREST MM DD YY [2.045] [2.038]	ORI CONTRIBUTOR [2.073] ADDRESS REPLY YES <input type="checkbox"/> DESIRED? [1.04]: CAR=Checked/CNA=Not Checked
SEND COPY TO: (ENTER ORI) [2.007]	DATE OF OFFENSE MM DD YY [2.752]	PLACE OF BIRTH (STATE OR COUNTRY) [2.020]	COUNTRY OF CITIZENSHIP [2.021]
MISCELLANEOUS NUMBERS [2.017]	SCARS, MARKS, TATTOOS, AND AMPUTATIONS [2.753 #1] SMT SET (SMT / SMTD) [2.753 #2] SMT SET (SMT / SMTD) [2.753 #3] SMT SET (SMT / SMTD)		
RESIDENCE / COMPLETE ADDRESS [2.041]		CITY	STATE
OFFICIAL TAKING FINGERPRINTS (NAME OR NUMBER) [2.480] OTP SET (OFN / ONT / OID)	LOCAL IDENTIFICATION / REFERENCE [2.009]		PHOTO AVAILABLE YES [2.036] PALM PRINTS TAKEN YES [2.035]
EMPLOYER: IF U.S. GOVERNMENT, INDICATE SPECIFIC AGENCY IF MILITARY, LIST BRANCH OF SERVICE AND SERIAL NO. [2.039]		OCCUPATION [2.040]	
CHARGE / CITATION 1. [2.752 #1] AOS SET (SEQ / OFC / OFL / COM / DOO / ATT / SOL / CSP / CMP / PRZ / SXM / FRM / WPN / DMV / DRG / DUI / ORA / OIN / DRA / WAR / TAA / RCC / FTA)		DISPOSITION 1. [2.752 #1] DRP / DOD / DST	
2. [2.752 #2] AOS SET (SEQ / OFC / OFL / COM / DOO / ATT / SOL / CSP / CMP / PRZ / SXM / FRM / WPN / DMV / DRG / DUI / ORA / OIN / DRA / WAR / TAA / RCC / FTA)		2. [2.752 #2] DRP / DOD / DST	
3. [2.752 #3] AOS SET (SEQ / OFC / OFL / COM / DOO / ATT / SOL / CSP / CMP / PRZ / SXM / FRM / WPN / DMV / DRG / DUI / ORA / OIN / DRA / WAR / TAA / RCC / FTA)		3. [2.752 #3] DRP / DOD / DST	
ADDITIONAL [2.752 #4] AOS SET (SEQ / OFC / OFL / COM / DOO / ATT / SOL / CSP / CMP / PRZ / SXM / FRM / WPN / DMV / DRG / DUI / ORA / OIN / DRA / WAR / TAA / RCC / FTA)		[2.752 #4] DRP / DOD / DST	
ADDITIONAL INFORMATION / BASIS FOR CAUTION If counts>4 Note:nnnadditional charges available"] [2.056]		STATE BUREAU STAMP Central Sites: PRINT OUT SITE SPECIFIC ADDRESS	
 PCN: [2.751]		* U.S. GPO: 1997 432-177/60018	

5.6.14 Washington Specific Template – Department of Corrections Card

5.6.14.1 Text placement on Federal Criminal fingerprint (FD-249) card (8 inches x 8 inches pre-printed), front side:

LEAVE BLANK CRIMINAL  TCN: [1.09]		(STAPLE HERE) <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <small>NFF SECOND SUBMISSION APPROXIMATE CLASS AMPUTATION SCAR</small>			LEAVE BLANK			
STATE USAGE		LAST NAME, FIRST NAME, MIDDLE NAME, SUFFIX [2.018]						
SIGNATURE OF PERSON FINGERPRINTED		SOCIAL SECURITY NO. [2.016]		LEAVE BLANK				
ALIASES/MAIDEN LAST NAME, FIRST NAME, MIDDLE NAME, SUFFIX [2.019 #1] [2.019 #2] [2.019 #3]		[2.022 #1] (DOB Alias) [2.022 #2] (DOB Alias) [2.022 #3] (DOB Alias)						
FBI NO. [2.014]	STATE IDENTIFICATION NO. [2.015]	DATE OF BIRTH MM DD YY [2.022]	SEX [2.024]	RACE [2.025]	HEIGHT [2.027]	WEIGHT [2.029]	EYES [2.031]	HAIR [2.032]
[2.084] #1 (AMP/FGP/AMPCD) [H.RT] <small>1. R. THUMB</small>	[2.084] #2 (AMP/FGP/AMPCD) [H.RI] <small>2. R. INDEX</small>	[2.084] #3 (AMP/FGP/AMPCD) [H.RM] <small>3. R. MIDDLE</small>	[2.084] #4 (AMP/FGP/AMPCD) [H.RR] <small>4. R. RING</small>	[2.084] #5 (AMP/FGP/AMPCD) [H.RL] <small>5. R. LITTLE</small>				
[2.084] #6 (AMP/FGP/AMPCD) [H.LT] <small>6. L. THUMB</small>	[2.084] #7 (AMP/FGP/AMPCD) [H.LI] <small>7. L. INDEX</small>	[2.084] #8 (AMP/FGP/AMPCD) [H.LM] <small>8. L. MIDDLE</small>	[2.084] #9 (AMP/FGP/AMPCD) [H.LR] <small>9. L. RING</small>	[2.084] #10 (AMP/FGP/AMPCD) [H.LL] <small>10. L. LITTLE</small>				
[2.067.1][2.067.2] SCANNER ID [H.L4] <small>LEFT FOUR FINGERS TAKEN SIMULTANEOUSLY</small>	[2.067.3] SCANNER S/N [2.038] [2.481]	[Current PRINTER S/N] (Actual Printer, Not Stored)	[Current DATE:TIME]	[H.LTP] [H.RTP] <small>L. THUMB R. THUMB</small>				
				[H.R4] <small>RIGHT FOUR FINGERS TAKEN SIMULTANEOUSLY</small>				

5.6.14.2 Text placement on Federal Criminal fingerprint (FD-249) card (8 inches x 8 inches pre-printed), rear side:

FEDERAL BUREAU OF INVESTIGATION, UNITED STATES DEPARTMENT OF JUSTICE WASHINGTON, D.C. 20537			
<small>PRIVACY ACT OF 1974 (P.L. 93-579) REQUIRES THAT FEDERAL, STATE, OR LOCAL AGENCIES INFORM INDIVIDUALS WHOSE SOCIAL SECURITY IS REQUESTED WHETHER SUCH DISCLOSURE IS MANDATORY OR VOLUNTARY. BASIS OF AUTHORITY FOR SUCH SOLICITATION AND USES WHICH WILL BE MADE OF IT.</small>			
JUVENILE FINGERPRINT SUBMISSION YES <input type="checkbox"/> TREAT AS ADULT YES <input type="checkbox"/>		DATE OF ARREST MM DD YY [2.045] (Intake Date) [2.038]	ORI CONTRIBUTOR [2.073] ADDRESS REPLY DESIRED? YES <input type="checkbox"/>
SEND COPY TO: (ENTER OR) [2.007]	DATE OF OFFENSE MM DD YY [2.752]	PLACE OF BIRTH (STATE OR COUNTRY) [2.020]	COUNTRY OF CITIZENSHIP [2.021]
MISCELLANEOUS NUMBERS [2.017]	SCARS, MARKS, TATTOOS, AND AMPUTATIONS [2.753 #1] SMT SET (SMT / SMTD) [2.753 #2] SMT SET (SMT / SMTD) [2.753 #3] SMT SET (SMT / SMTD)		
	RESIDENCE / COMPLETE ADDRESS [2.041]	CITY	STATE
OFFICIAL TAKING FINGERPRINTS (NAME OR NUMBER) [2.480] OTP SET (OFN / ONT / OID)	LOCAL IDENTIFICATION / REFERENCE [2.009] DOC #)		PHOTO AVAILABLE YES <input type="checkbox"/> [2.036] PALM PRINTS TAKEN YES <input type="checkbox"/> [2.035]
EMPLOYER: IF U.S. GOVERNMENT, INDICATE SPECIFIC AGENCY IF MILITARY, LIST BRANCH OF SERVICE AND SERIAL NO. [2.039]	OCCUPATION [2.040]		
CHARGE / CITATION ¹ [2.781] DAS SET (SEQ/OFC/OFL/COM/DOO/STA/CCO/ATT/SOL/CSP/CMP/PRZ/SXM/FRM/WPN/DMV/DRG/DUI/RCC)		DISPOSITION ¹ [2.051] #1 CSL SET (CPL/CDD)	
² [2.781] DAS SET (SEQ/OFC/OFL/COM/DOO/STA/CCO/ATT/SOL/CSP/CMP/PRZ/SXM/FRM/WPN/DMV/DRG/DUI/RCC)		² [2.051] #2 CSL SET (CPL/CDD)	
³ [2.781] DAS SET (SEQ/OFC/OFL/COM/DOO/STA/CCO/ATT/SOL/CSP/CMP/PRZ/SXM/FRM/WPN/DMV/DRG/DUI/RCC)		³ [2.051] #3 CSL SET (CPL/CDD)	
ADDITIONAL [if counts >4 NOTE: "nnn additional counts available"] [2.781] DAS SET (SEQ/OFC/OFL/COM/DOO/STA/CCO/ATT/SOL/CSP/CMP/PRZ/SXM/FRM/WPN/DMV/DRG/DUI/RCC)		[2.051] #4 CSL SET (CPL/CDD)	
ADDITIONAL INFORMATION / BASIS FOR CAUTION If counts >4 Note: nnn additional charges available"] [2.056]		STATE BUREAU STAMP Central Sites: PRINT OUT SITE SPECIFIC ADDRESS	


5.6.15 Washington Specific Template – Applicant

5.6.15.1 Text and image placement on Federal Applicant fingerprint (FD-258) card (8 inches x 8 inches pre-printed), front (images) side only:

APPLICANT		LEAVE BLANK TCN: [1.09]		TYPE OR PRINT ALL INFORMATION IN BLACK LAST NAME NAM FIRST NAME MIDDLE NAME				FBI LEAVE BLANK	
SIGNATURE OF PERSON FINGERPRINTED		ALIAS AKA [2.019 #1] [2.019 #2] [2.019 #3]		O R I [2.073]				DATE OF BIRTH DOB MONTH DAY YEAR [2.022]	
RESIDENCE OF PERSON FINGERPRINTED [2.041]		CITIZENSHIP CTZ [2.021]		SEX [2.024]	RACE [2.025]	HGT [2.027]	WGT [2.029]	EYES [2.031]	HAIR [2.032]
DATE [2.038]	SIGNATURE OF OFFICIAL TAKING FINGERPRINTS [2.480] OTP SET (OFN / ONT / OID)		YOUR NO. OCA [2.009]		LEAVE BLANK				
EMPLOYER AND ADDRESS [2.039]		FBI NO. FBI [2.014]		ARMED FORCES NO. MNU		CLASS _____			
REASON FINGERPRINTED [2.037]		SOCIAL SECURITY NO. [2.016]		MISCELLANEOUS NO. MNU [2.017]		REF _____			
[2.084] #1 (AMP/FGP/AMPCD) [H.RT]		[2.084] #2 (AMP/FGP/AMPCD) [H.RI]		[2.084] #3 (AMP/FGP/AMPCD) [H.RM]		[2.084] #4 (AMP/FGP/AMPCD) [H.RR]		[2.084] #5 (AMP/FGP/AMPCD) [H.RL]	
1. R. THUMB		2. R. INDEX		3. R. MIDDLE		4. R. RING		5. R. LITTLE	
[2.084] #6 (AMP/FGP/AMPCD) [H.LT]		[2.084] #7 (AMP/FGP/AMPCD) [H.LI]		[2.084] #8 (AMP/FGP/AMPCD) [H.LM]		[2.084] #9 (AMP/FGP/AMPCD) [H.LR]		[2.084] #10 (AMP/FGP/AMPCD) [H.LL]	
6. L. THUMB		7. L. INDEX		8. L. MIDDLE		9. L. RING		10. L. LITTLE	
[2.067.1] Scanner ID	[2.067.2] Scanner S/N	[2.067.3] Scanner S/N	[2.038] [2.481]	[PALETTE TARGETS] (actual printer, not stored)		[CURRENT PRINTER S/N] (actual Printer, not stored)		[Current DATE:TIME] CCYYMMDD:HHMM	
[H.L4]		[H.LTP]	[H.RTP]	[H.R4]					
LEFT FOUR FINGERS TAKEN SIMULTANEOUSLY				L THUMB	R THUMB	RIGHT FOUR FINGERS TAKEN SIMULTANEOUSLY			

5.6.16 Washington Specific Template – Personal Identification


5.6.16.1 Text and image placement on Federal Personal Identification fingerprint (FD-353) card (8 inches x 8 inches pre-printed), front (images) side only:

 SEE TCN: 1.09 FOR FURTHER INSTRUCTIONS		PERSONAL IDENTIFICATION TYPE OR PRINT ALL INFORMATION IN BLACK LAST NAME <u>NAM</u> FIRST NAME _____ MIDDLE NAME _____ [2.018]			FBI: LEAVE BLANK		
SIGNATURE OF PERSON FINGERPRINTED _____		FINGERPRINTS SUBMITTED BY _____			DATE OF BIRTH <u>DOB</u> Month _____ Day _____ [2.022]		
RESIDENCE OF PERSON FINGERPRINTED _____ [2.041]		DATE FINGERPRINTED [2.038]		SEX <u>[2.024]</u>	RACE <u>[2.025]</u>	HGT <u>[2.027]</u>	
PERSON TO BE NOTIFIED IN CASE OF EMERGENCY		SOCIAL SECURITY NO. [2.016]		WGT <u>[2.029]</u>	EYES <u>[2.031]</u>	HAIR <u>[2.032]</u>	
NAME _____		MISCELLANEOUS NO. _____		PLACE OF BIRTH <u>POB</u> [2.020]			
ADDRESS _____		SCARS AND MARKS [2.753] SMT SET (SMT / SMTD)		CLASS _____			
FINGERPRINTED BY [2.480] OTP SET (OFN/ONT/OID)		REF. _____		2.015			
[2.084] #1 AMP/FGP/AMPCD [H.RT] <small>1. R. THUMB</small>		[2.084] #2 AMP/FGP/AMPCD [H.RI] <small>2. R. INDEX</small>		[2.084] #3 AMP/FGP/AMPCD [H.RM] <small>3. R. MIDDLE</small>		[2.084] #4 AMP/FGP/AMPCD [H.RR] <small>4. R. RING</small>	
[2.084] #5 AMP/FGP/AMPCD [H.RL] <small>5. R. LITTLE</small>		[2.084] #6 AMP/FGP/AMPCD [H.LT] <small>6. L. THUMB</small>		[2.084] #7 AMP/FGP/AMPCD [H.LI] <small>7. L. INDEX</small>		[2.084] #8 AMP/FGP/AMPCD [H.LM] <small>8. L. MIDDLE</small>	
[2.084] #9 AMP/FGP/AMPCD [H.LR] <small>9. L. RING</small>		[2.084] #10 AMP/FGP/AMPCD [H.LL] <small>10. L. LITTLE</small>		[2.067.1][2.067.2] SCANNER ID		[2.067.3] SCANNER S/N	
[2.038] [2.481]		[Current PRINTER S/N] (Actual Printer, Not Stored)		[Current DATE:TIME]		[H.L4]	
<small>LEFT FOUR FINGERS TAKEN SIMULTANEOUSLY</small>		<small>L. THUMB</small>		<small>R. THUMB</small>		<small>RIGHT FOUR FINGERS TAKEN SIMULTANEOUSLY</small>	

Note: Used when Tag 2.037 equals “PERSONAL IDENTIFICATION”

5.6.17 Washington Specific Template – Sex / Kidnapping Offender Registration

5.6.17.1 Text and image placement on Washington State Sex / Kidnapping Offender Registration fingerprint (3000-240-535) card (8 inches x 8 inches pre-printed), front (images) side:

LEAVE BLANK  TCN: [1.09]		SEX/KIDNAPPING OFFENDER REGISTRATION [2.756] TYPE OF REGISTRATION <input type="checkbox"/> SEX OFFENDER REGISTRATION <input type="checkbox"/> KIDNAPPING OFFENDER REGISTRATION <input type="checkbox"/> SEX/KIDNAPPING OFFENDER REGISTRATION				LEAVE BLANK		
STATE USAGE		LAST NAME, FIRST NAME, MIDDLE NAME, SUFFIX [2.018]						
SIGNATURE OF PERSON FINGERPRINTED		SOCIAL SECURITY NUMBER [2.016]		LEAVE BLANK				
ALIASES/MAIDEN LAST NAME, FIRST NAME, MIDDLE NAME, SUFFIX [2.019] #1 [2.022] #1 (DOB Alias) [2.019] #2 [2.022] #2 (DOB Alias) [2.019] #3 [2.022] #3 (DOB Alias)		INFORMATION PROVIDED ON THIS CARD MAY BE COMPUTERIZED IN LOCAL, STATE AND FEDERAL FILES						
FBI NO. [2.014]	STATE IDENTIFICATION NO. [2.015]	DATE OF BIRTH: MMDDYY [2.022]	SEX [2.024]	RACE [2.025]	HEIGHT [2.027]	WEIGHT [2.029]	EYES [2.031]	HAIR [2.032]
[2.084] #1 AMP/FGP/AMPCD [H.RT]	[2.084] #2 AMP/FGP/AMPCD [H.RI]	[2.084] #3 AMP/FGP/AMPCD [H.RM]	[2.084] #4 AMP/FGP/AMPCD [H.RR]		[2.084] #5 AMP/FGP/AMPCD [H.RL]			
<small>1. R. THUMB</small>	<small>2. R. INDEX</small>	<small>3. R. MIDDLE</small>	<small>4. R. RING</small>		<small>5. R. LITTLE</small>			
[2.084] #6 AMP/FGP/AMPCD [H.LT]	[2.084] #7 AMP/FGP/AMPCD [H.LI]	[2.084] #8 AMP/FGP/AMPCD [H.LM]	[2.084] #9 AMP/FGP/AMPCD [H.LR]		[2.084] #10 AMP/FGP/AMPCD [H.LL]			
<small>6. L. THUMB</small>	<small>7. L. INDEX</small>	<small>8. L. MIDDLE</small>	<small>9. L. RING</small>		<small>10. L. LITTLE</small>			
[2.067.1][2.067.2] SCANNER ID	[2.067.3] SCANNER S/N	[2.038] [2.481]	[Current PRINTER S/N] (Actual Printer, Not Stored)		[Current DATE:TIME]			
[H.L4]	[H.LTP]	[H.RTP]	[H.R4]					
<small>LEFT FOUR FINGERS TAKEN SIMULTANEOUSLY</small>		<small>L. THUMB</small>	<small>R. THUMB</small>	<small>RIGHT FOUR FINGERS TAKEN SIMULTANEOUSLY</small>				

5.6.17.2 Text placement on Washington State Sex / Kidnapping Offender Registration fingerprint (3000-240-535) card (8 inches x 8 inches pre-printed), rear side:

WASHINGTON STATE PATROL IDENTIFICATION AND CRIMINAL HISTORY SECTION			
P.O. BOX 42633 OLYMPIA, WA 98504-2633			
<p>PRIVACY ACT OF 1974 (PL. 93-579) REQUIRES THAT FEDERAL, STATE, OR LOCAL AGENCIES INFORM INDIVIDUALS WHOSE SOCIAL SECURITY NUMBER IS REQUESTED WHETHER SUCH DISCLOSURE IS MANDATORY OR VOLUNTARY, BASIS OF AUTHORITY FOR SUCH SOLICITATION, AND USES WHICH WILL BE MADE OF IT.</p>			
<p>INSTRUCTIONS</p> <p>1. REGISTRATION SUBMISSION REQUIRES SOR REGISTRATION FINGERPRINT CARD AND A PHOTOGRAPH, PURSUANT TO RCW 9A.44.130. 2. SHERIFF'S OFFICE MUST SUBMIT REGISTRATION TO THE WASHINGTON STATE PATROL WITHIN 5 DAYS. 3. ON BACK OF PHOTOGRAPH, INCLUDE REGISTRANT'S NAME AND DOB.</p>			
<p>WHO MUST REGISTER</p> <p>ANY INDIVIDUAL IN THIS STATE WHO HAS BEEN FOUND TO HAVE COMMITTED OR HAS BEEN CONVICTED OF ANY SEX OFFENSE OR KIDNAPPING OFFENSE, OR WHO HAS BEEN FOUND NOT GUILTY BY REASON OF INSANITY UNDER CHAPTER 10.77 RCW, AS DESCRIBED IN RCW 9A.44.130.</p>			
<p>REASON FOR REGISTRATION:</p> <p><input type="checkbox"/> RESIDENT [2.757] RFR SET (RFR / RFN)</p> <p><input type="checkbox"/> NON-RESIDENT</p> <p><input type="checkbox"/> EMPLOYMENT</p> <p><input type="checkbox"/> STUDENT</p> <p>"X" in appropriate box</p>	<p>REGISTRATION DATE:</p> <p>[2.758]</p> <p>ENDING REGISTRATION DATE:</p> <p>[2.759]</p>	<p>ORI:</p> <p>CONTRIBUTOR: [2.073]</p> <p>ADDRESS:</p>	
<p>RISK LEVEL CLASSIFICATION:</p> <p>[2.760] <input type="checkbox"/> I <input type="checkbox"/> II <input type="checkbox"/> III <input type="checkbox"/> IV</p> <p>"X" in appropriate box</p>	<p>DATE OF CONVICTION:</p> <p>[2.761] (NCRR)</p> <p>[2.762] (CRR)</p>	<p>PLACE OF BIRTH (STATE OR COUNTRY):</p> <p>[2.020]</p>	<p>COUNTRY OF CITIZENSHIP:</p> <p>[2.021]</p>
<p>PLACE OF CONVICTION:</p> <p>[2.763]</p>	<p>SCARS, MARKS, TATTOOS, AND AMPUTATIONS:</p> <p>[2.753] #1 SMT SET (SMT / SMTD)</p> <p>[2.753] #2 SMT SET (SMT / SMTD)</p> <p>[2.753] #3 SMT SET (SMT / SMTD)</p>		
<p>CONVICTION(S) RESULTING IN REGISTRATION:</p> <p>[2.761] (NCRR)</p>	<p>[2.762] (CRR)</p>	<p>SEXUAL PREDATOR:</p> <p>[2.764]</p> <p>"X" if appropriate box</p>	<p>DNA AVAILABLE:</p> <p>[2.765]</p> <p>"X" if appropriate box</p>
<p>OF WA STATE OR OTHER STATES:</p> <p>[2.480] OTP SET (OFN/ONT/OID)</p>	<p>LOCAL IDENTIFICATION NUMBER:</p> <p>[2.009]</p>	<p>CAUTION AND MEDICAL CONDITIONS:</p> <p>[2.766]</p>	
<p>CURRENT RESIDENCE OF PERSON BEING FINGERPRINTED</p>			
<p>[2.767]</p> <p>STREET ADDRESS:</p> <p>[2.769]</p>			
<p>CITY:</p> <p>[2.769]</p>	<p>STATE:</p> <p>[2.770]</p>	<p>ZIP CODE:</p> <p>[2.771]</p>	<p>PHONE NO.:</p> <p>[2.772]</p>
<p>OCCUPATION:</p> <p>[2.040]</p>	<p>EMPLOYER:</p> <p>[2.773]</p>	<p>EMPLOYER STREET ADDRESS:</p> <p>[2.774]</p>	
<p>EMPLOYER CITY:</p> <p>[2.775]</p>	<p>STATE:</p> <p>[2.776]</p>	<p>ZIP CODE:</p> <p>[2.777]</p>	<p>PHONE NO.:</p> <p>[2.778]</p>
<p>ADDITIONAL INFORMATION</p> <p>[2.056]</p>		<p>LEAVE BLANK</p>	
<p>3000-240-535 (R 7/99)</p>			

5.7 Attachment G - Print Server Site Preparation Specifications

5.7.1 Power Requirements

- 1 110v outlet print server (2 amps)
- 1 110v outlet monitor 15/17/18 in. (.8-1.2 amp)
- 1 110v outlet double-sided printer (7 amps)
- 1 15-amp circuit required

5.7.2 Equipment Specifications

- 1 15" Monitor LCD H-13.87" W 13.54" D-5.3"
- 1 17" Monitor LCD H-14.9" W 14.9" D-5.6"
- 1 Print Server Base Unit (Tower) H-17" W-8" D-17"
- 1 Print Server Base Unit H-5" W-15" D-10"
- 1 Keyboard
- 1 Mouse PS2 compatible
- 1 Double-Sided card printer with hopper

5.7.3 Network Requirement

- 1 IP address required
- 1 CAT5 RJ45 connection cable

5.7.4 Environment Required

- Normal office environment
- All Equipment specifications may vary based on availability, equipment type, and model.

5.8 Attachment H – WIN Member State FBI Submission ORI Table

Table 5-1 WIN ORI TABLE

Revised July 16, 2008

AGENCY	TENPRINT	LATENT
Alaska	AK020065Y	AK020075Y
IDAHO	ID001085Y	ID001095Y
MONTANA	MT025405Y	MT025415Y
NEVADA	NV0131713	NV0132000
OREGON	OR0SBI100	OR0SBI200
UTAH	UTBCI0099	UTBCI0098
WASHINGTON STATE	WAWSP0100	WAWSP0200
WYOMING	WY0111400	WY0112400
BICE	CAINS0100	
FBI IAFIS	WVIAFIS0Z	
WIN	CA034019Y	CA034029Y
WIN TEST	CA034039Y	

5.8.1 Attachment I - NEC AFIS Workstation and Associated Peripheral Equipment Installation Site Survey

5.8.1.1 WIN Equipment / Network Site survey

Site Name: _____

The following is a list to go by to help ask the right questions. We want to make sure we cover all the bases.

STATE is responsible for local wire installation and maintenance. These are just guidelines to make sure all installations conform to set standards and will make for a clean and stable network.

Security

Please describe below how the device will be installed to meet WIN and FBI/CJIS Network Management and Security Policy.

Location

Does site need any sort of preparation before FW install? _____

If yes, please explain: _____

If remodeling, please list completion dates: _____

Where is it intended to place network equipment? _____

Is location secure, in that the general public does not have access to network equipment? _____

How far from the WIN GFW's will network HUB/Switch and router be? _____

Please describe the distance and facility where GFW's will be installed. _____

Are they able to connect to State WAN? _____

(Disregard above WAN question if at Central Site)



Power Requirements

How many power receptacles are going to be necessary? _____

Are they available now? _____

If network equipment will reside in communication closet, is there enough power for it? _____

Is UPS/BBU currently available? _____

Will it be available to support new equipment? _____

Quantities

How many WIN GFW's will be installed? _____

How many B/W printers will be installed? _____

Networked _____ Local (connected to GFW) _____

Network Install

Is there local business' that can install and certify CAT 5/UTP for data trans. speeds up to 100Mbps? _____

Does any cabling need to go in ceiling? _____ Under floors? _____

Through walls? _____

If in the ceiling, cabling should be PLENUM, and should also be solid core for the long runs from patch panel to outlet. From outlet a flexible stranded core PATCH cord is the most desirable.

Cable ends should be terminated in standardized wall outlets, certified for CAT 5. Wherever possible, the solid core cabling should be hidden in a wall, desk jack, and cable pole, whatever to limit its movement. There are numerous considerations for installing CAT 5 but that is beyond the scope of this survey.

From the termination point or outlet a high quality stranded CAT 5 cable will provide the best flexibility for connections that tend to MOVE a lot at the backs of the terminals.

It is absolutely imperative all cabling is standard and marked well, can this be accomplished?

Are there any considerations to get to COMM/Closet if that is where network equipment will be housed? _____

It is most desirable to have a separate cable run for each terminal, network printer, etc. If absolutely necessary, a high quality MINI HUB can be utilized to forego having to install numerous extra cables.

What distance are we looking at if a separate run is necessary? _____

Dates

What are the expected installation dates for:

➤ PHONE LINES? _____

➤ NETWORK?

➤ HUB/SWITCH?

➤ ROUTER?

Point of Contact



5.8.1.2 Equipment -- Power requirements -- Workstations and peripheral devices

NEC recommends that all equipment be on UPS power either small local units or larger units, which traditionally provide power in a computer room environment. Depending on the equipment you have, the following are power requirements and equipment specifications.

1 ea. Fingerprint Workstations – Tenprint / Latent

110V	Workstation Base Unit (tower)	8”w x 17”h x 18.5”d	4.5 amps
	Keyboard	18.5” w x 2.5”h x 7.5”d	Mouse - PS2
110V	Monitor - 21” flat screen	20”w x 15.5”h x 7.9”d	2.1 amps
110V	Desktop Scanner-full extension lid	14”w x 24”h x 24”d	1.3 amps
110V	Compact Scanner (Latent only)	13”w x 20”h x 21”d	1.4 amps
110V	B&W laser printer	16”w x 14”h x 18”d	4.0 amps

5.8.1.2.1 Network Requirement

- 1 IP address required for W/S
- 1 CAT5 RJ45 connection cable

- 1 IP address required, if networked printer
- 1 CAT5 RJ45 connection cable

5.8.1.2.2 Environment Required

Normal office environment

Note: All Equipment specifications may vary based on availability, equipment type, and model.
All Equipment conforms to NEMA-5-15R

5.8.1.3 Recommended Cabling Practices

Do's:

- Use connecting hardware that is compatible with the installed cable.
- Terminate each horizontal cable on a dedicated telecommunications outlet.
- Maintain the twist of horizontal and backbone cable pairs up to the point of termination.
- Tie and dress cables neatly not exceeding the minimum bend radius.
- Place cabling at a sufficient distance from equipment that may generate high levels of electromagnetic interference.

Don'ts:

- Do not use connecting hardware that is of a lower category than the cable being used.
- Do not create multiple appearances of the same cable at several distribution points (called bridged taps).
- Do not locate cross-connects where cable distances will exceed the maximum.
- Do not leave any wire pairs untwisted.
- Do not over-tighten cable ties or make sharp bends with cables.

Connector Terminations:

- Pair twists shall be maintained as close as possible to the point of termination.
- Untwisting shall not exceed 25 mm (1.0 in.) for category 4 links and 13 mm (0.5 in.) for category 5 links.
- Connecting hardware shall be installed to provide well-organized installation with cable Management and in accordance with manufacturer's guidelines.
- Strip back only as much jacket as is required to terminate individual pairs.
- From the termination point or outlet, a high quality stranded CAT 5 cable will provide the best flexibility for connections that tend to move such as the back of terminals.

UTP Patch Cords and Cross-connect Jumpers:

- Patch cords must use stranded cable for adequate flex-life.
- Patch cords must not exceed 3 meters.
- Must meet minimum performance requirements for horizontal cable except that twenty percent more attenuation is allowed for stranded cables.

Cabling Practices:

- Solid core Cat 5 cable should be used from Patch panel to terminal jack.
- To avoid stretching, pulling tension should not exceed 110N (25 lbf) for 4-pair cables.
- Any cabling in ceilings should be plenum and solid core for the long runs from the patch panel to the outlet. From the outlet, a flexible stranded core Patch cord is the most desirable.
- It is most desirable to have a separate cable run for each terminal or server.
- Cable ends should be terminated in standardized wall outlets, certified for CAT 5. Whenever possible, the solid core cabling should be hidden in a wall, desk jack or cable pole to limit its movement.
- Installed bend radii in spaces with UTP terminations shall not exceed:
 - Four times the cable diameter for horizontal UTP cables.
 - Ten times the cable diameter for multi-pair backbone UTP cables
- Avoid cable stress, as caused by:
 - Cable twist during pulling or installation
 - Tension caused by suspended cable runs
 - Tightly cinched cable ties
- Horizontal cables should be used with connecting hardware and patch cords (or jumpers) of category 5 or higher.

5.8.2 Premises Wiring Color Code

Table 5-2: Wiring Color Code

CONDUCTORS		
	EIA/TIA Standards Twisted Pair color coding	
RJ45 8 Pin		
T568B		
Pair 1		
	White Blue*	5
	Blue**	4
Pair 2		
	White-Orange*	1
	Orange**	2
Pair 3		
	White-Green*	3
	Green**	6
Pair 4		
	White-Brown*	7
	Brown**	8

Figure 5-4: Ethernet T568B Color Diagram

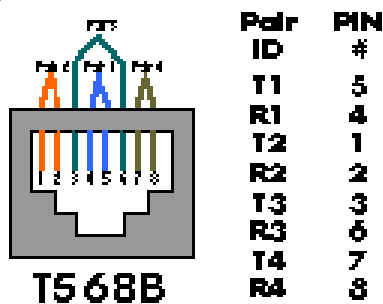
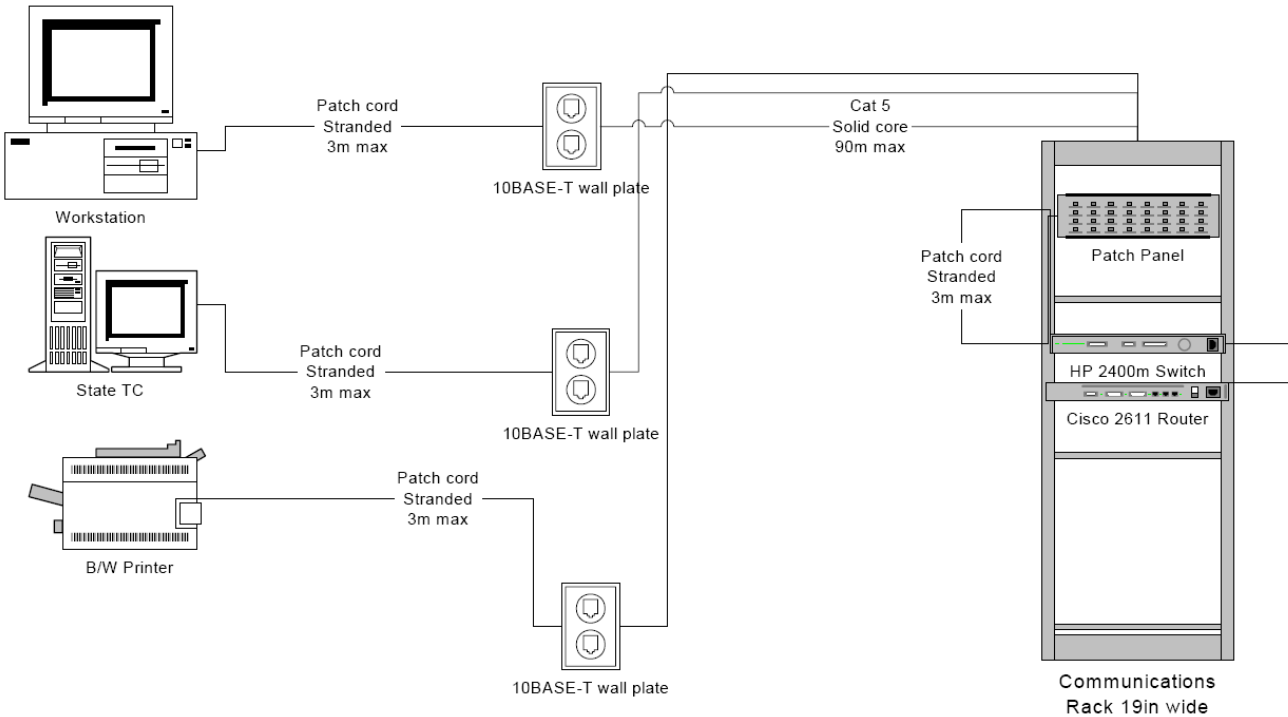


Table 5-3: Ethernet Base - Patch Cord Colors

ETHERNET 10 BASE – PATCH CORD (T568B COLORS)			
T2	1	White/Orange	1 TxData +
R2	2	Orange	2 Txa –
T3	3	White/Green	3 RecvData +
R1	4	Blue	4
T1	5	White/Blue	5
R3	6	Green	6 RecvData –
T4	7	White/Brown	7
R4	8	Brown	8

Figure 5-5: Network Diagram



5.9 Attachment J – FBI IAFIS Tenprint Connectivity Checklist

5.9.1 IAFIS Tenprint Connectivity Checklist

Please complete the attached checklist to inform of your agency's status of ten-print connectivity to the Integrated Automated Fingerprint Identification System (IAFIS).

State/Federal Agency: _____

Your agency's tenprint Technical Point of Contact (POC) for civil and criminal submissions:
(Criminal) _____

(Civil) _____

Phone number of Technical POCs:

(Criminal) _____

(Civil) _____

Your agency's Analyst POC for civil and criminal submissions:

(Criminal) _____

(Civil) _____

Phone number of Analyst POCs:

(Criminal) _____

(Civil) _____

Your agency's 24 hour POC for civil and criminal submissions:

(Criminal) _____

(Civil) _____

Phone number of 24 hour POCs:

(Criminal) _____

(Civil) _____

When do you anticipate testing with IAFIS? _____

What volume of civil and criminal electronic ten-print submissions do you anticipate submitting on your day one connection? _____

(Criminal) _____

(Civil) _____

What is your host registered IP address? _____

What is your IP address and Submask for the CJIS Router? _____

➤ IP Address _____

➤ Submask _____

Does your agency use any other routers or firewalls between your host AFIS and the FBI remote router? _____

If yes, what registered IP address and Submask will be used for that router or firewall? _____

➤ IP Address _____

➤ Submask _____

What fully qualified host domain name will your agency be using? _____

What email address will your agency be using for responses? (SRE & ERRT) _____

What originating agency identifier (ORI) number will your agency be using for your ten-print IAFIS electronic submissions? _____

Would your agency like to be provided with a Points of Contact list in states that are already submitting electronically to IAFIS? _____

Is your agency interested in having the Identification and Investigative Services Section perform a three week study on your state's current rejection problems to assist you in your electronic ten-print connectivity?

5.10 Attachment K - FBI IAFIS Latent Connectivity Checklist

5.10.1 Latent Connectivity Checklist

Please complete this checklist to inform of your agency's plan for remote latent connectivity to the Integrated Automated Fingerprint Identification System (IAFIS).

State Agency: _____

Your state's latent connectivity Coordinator: _____

Phone Number of Coordinator: _____

What is your agency's tentative date for submitting remote latent searches to IAFIS? _____

Has your agency acquired a remote latent workstation? _____

If yes, what type of workstation will your agency be using? (I.E, Universal Latent Workstation or state AFIS connected workstation) _____

Is your agency interested in receiving information regarding the Universal Latent Workstation? _____

Please note that if your latent management system is not resident on your state store and forward or you are connecting via a Laboratory CJIS WAN connection, your state will need to provide the FBI with a separate registered IP address, Submask and domain name.

Registered IP address: _____

Domain Name: _____

Submask: _____

Does your agency use any other routers or firewalls between your host AFIS and the FBI remote router? _____

If yes, what registered IP address and Submask will be used for that router or firewall? _____

➤ IP Address _____

➤ Submask _____

What email address will your agency be using for responses? (SRE & ERRT) _____

Please provide any additional information or questions your agency has regarding your remote latent connection to IAFIS?

Please fax or mail this survey to your Systems Transition Unit Regional Representative. The fax number is (304) 625-3875. Your Regional Representative's address is:

FBI CJIS Division

1000 Custer Hollow Road Clarksburg, West Virginia 26306

Attention (Regional Representative), Module C-3

Western Region

Julia Minnocci (304) 625-5243

Jminnoc1@leo.gov

Federal Region

Garnet Tucker (304) 625-3543

gtucker@leo.gov

Your regional representative will be contacting you to discuss the survey and to provide any additional information you requested.



NEC Corporation of America
Biometrics Solutions Division
10850 Gold Center Drive, Suite 200
Rancho Cordova, CA 95670

Toll-Free: 800.777.AFIS
Locally: 916.463.7000
Fax: 916.463.7041

Email: idsolutions@necam.com
On the web: www.necam.com/ids/afis

**WASHINGTON STATE PATROL
LIVE-SCAN TO WESTERN IDENTIFICATION NETWORK AUTOMATED BIOMETRIC
IDENTIFICATION SYSTEM (WIN ABIS) CONNECTION USER'S AGREEMENT**

THIS AGREEMENT, entered into between the Washington State Patrol (hereinafter referred to as "WSP"), an agency of the State of Washington; and the Ruston Police Department, (hereinafter referred to as "the User"), witnesses that:

1. WSP is an agency of the State of Washington authorized by law to establish and operate an Automated Biometric Identification System (hereinafter referred to as "ABIS") capable of, but not limited to, reading, classifying, matching, and storing fingerprints, and to maintain criminal history record information based on fingerprint identification. ABIS is a state-funded system comprised of a central computer processor located at the WSP in Olympia. The criminal history repository is known as the Washington State Identification System (WASIS) and maintained by WSP in Olympia.
2. WSP has entered into agreement with the Western Identification Network (WIN) for ABIS services. The WIN ABIS is a multi-state funded system comprised of a host system presently located in Rancho Cordova, California (the WIN Central Site) with remote input stations and booking terminals in member states as authorized by the WIN Board of Directors.
3. The User operates live-scan fingerprinting equipment to capture fingerprint images and related information of a person arrested, registering as a sex or kidnapping offender, applying for licensing or employment pursuant to state or local requirements ("Applicant Submissions"), or as required for the emergency placement of children pursuant to the Adam Walsh Child Protection and Safety Act of 2006, Section 151.

NOW THEREFORE, in light of the foregoing representations and the promises, conditions, and other valuable considerations more fully set out or incorporated herein by reference, the parties, by their duly authorized officials, do mutually agree as follows:

1. WSP will furnish the User, a criminal justice agency as defined in chapter 10.97 RCW, with such criminal justice information as is available in WASIS, ABIS and WIN ABIS files. WSP will serve as the means of exchange of computerized criminal history information and fingerprint data.
2. The network connection will be made via an e-mail server administered by WSP. This network and local networks will meet the requirements of Criminal Justice Information Services (CJIS) Security Policy. The User shall notify WSP of sustained or repeated network problems that affect this service.
3. The User will submit the fingerprint images and the related information electronically to the WSP for the purpose of identification and, when applicable, inclusion in the ABIS, WASIS and WIN ABIS databases. For Applicant Submissions requiring a fee, the User agrees to establish a fingerprint services billing account with WSP. By establishing a billing account for fingerprint image submissions, the User agrees to collect, hold, and reconcile fees charged by WSP for the type of applicant fingerprints submitted by the User. If a transmission is sent in error, the User is still responsible for all fees associated with the transaction type.

4. The User agrees that WSP will provide authorization for access to the ABIS, WASIS and WIN ABIS databases with certain restrictions depending on system capabilities and assigned status as follows:
 - A. Local live-scan sites will submit fingerprint images and related information for identification search and inclusion in the ABIS, WASIS and WIN ABIS databases.
 - B. The User agrees to comply with statutory mandates concerning the submission of criminal and civil fingerprint submissions to WSP.
5. The User agrees that only the WSP site or authorized remote sites may permanently register fingerprints into the ABIS, WASIS and WIN ABIS databases.
6. The WSP ABIS Coordinator or designee will provide the User with policies including, but not limited to, a schedule for accessing the ABIS, WASIS and WIN ABIS databases. Such policies shall define the basis and procedures for conducting routine and emergency comparison of fingerprints against these databases.
7. The User shall take necessary measures to make its live-scan equipment and system secure and prevent unauthorized use. WSP reserves the right to object to equipment security measures and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP.
8. Livescan equipment is the property of WSP and is on loan to the user. The User agrees to pay installation costs and purchase maintenance from the live-scan vendor for the loaned live-scan equipment for as long as the user utilizes the device.
9. The User agrees to assign a live-scan coordinator to serve as the primary contact person for the User in Live-Scan to ABIS connection-related issues. The User also agrees to notify WSP immediately, in writing, of any changes in this position.
10. WSP agrees to schedule and provide training of equipment and procedures to User personnel at locations and times arranged by WSP. Equipment operation training may be supplied by WSP or the equipment provider.
11. The User shall access and utilize ABIS, WASIS and WIN ABIS databases only in conjunction with the administration of criminal justice as authorized by laws governing criminal history dissemination.
12. Fingerprint identification or criminal history information records provided to the User under this Agreement shall not be further disseminated by the User to any other person or (private or public) entity, except as required in criminal proceedings or pursuant to state or federal law.

PERIOD OF PERFORMANCE

This Agreement becomes effective on the date of the last signature and continues until June 30, 2022 or until termination as provided herein.

COMPLIANCE WITH LAWS, REGULATIONS AND PROCEDURES

The User agrees to comply with all applicable federal and state laws, regulations, rules, and procedures, and to assume certain costs associated with the User's use of the services described herein. The User shall operate livescan equipment and otherwise conduct itself in strict compliance with applicable policies and procedures published by WIN and WSP including: the Policies and Procedures of WIN ABIS as currently in force; the Washington State Patrol (WSP) Access User Acknowledgment, and the policies and procedures identified in this Agreement.

The Policies and Procedures of WIN ABIS are hereby incorporated into and made a part of this Agreement except to the extent that they are inconsistent with anything found herein. The User will comply with related FBI Criminal Justice Information Services Security (CJIS) Policy and other security practices adopted by WIN as these relate to ABIS, WASIS and WIN ABIS.

SUSPENSION AND TERMINATION

WSP may suspend further performance of services hereunder when, in its reasonable estimation, the User has breached any material term of the Agreement. For the purposes of this Agreement, the violation of any specific term of this Agreement or of any substantive requirement or limitation imposed by the federal or state statutes, regulations, or rules incorporated into this Agreement shall be deemed a breach of a material term of the Agreement.

WSP may terminate this Agreement if the User commits any material breach of any term of this Agreement, which breach is not cured within thirty (30) business days after receipt of notice from WSP. Both parties may, by mutual agreement, terminate this Agreement on terms then acceptable to them.

Upon termination of this Agreement for any reason, each party shall promptly return to the other any property that belongs to the other party. With respect to hardware or software products that are the property of WSP or WIN, the User shall promptly return such property to WSP.

Neither WIN, WSP nor the User shall be liable for (i) any indirect, incidental, consequential or special damages under this agreement arising solely from the termination of this Agreement in accordance with its terms.

HOLD HARMLESS

The User agrees to hold harmless the Western Identification Network and its employees; and the State of Washington, the Washington State Patrol and its employees from and against any and all claims, demands, actions, suits, including but not limited to, any liability for damages by reason of or arising out of any misuse of the ABIS, WASIS and WIN ABIS databases, erroneous fingerprint identifications made by user personnel, or any cause of action whatsoever, and against any loss, cost, expense, and damage resulting therefrom, including attorney's fees.

This agreement replaces any previous agreement between WSP and the User on this subject.

IN WITNESS THEREOF, the duly authorized officials of the respective parties have executed this written Agreement.

RUSTON POLICE DEPARTMENT

WASHINGTON STATE PATROL

BY _____

TITLE _____

Simon Tee, Grants and Contracts Manager

DATE _____

APPROVED AS TO FORM BY THE OFFICE OF THE ATTORNEY GENERAL 6/2/2010