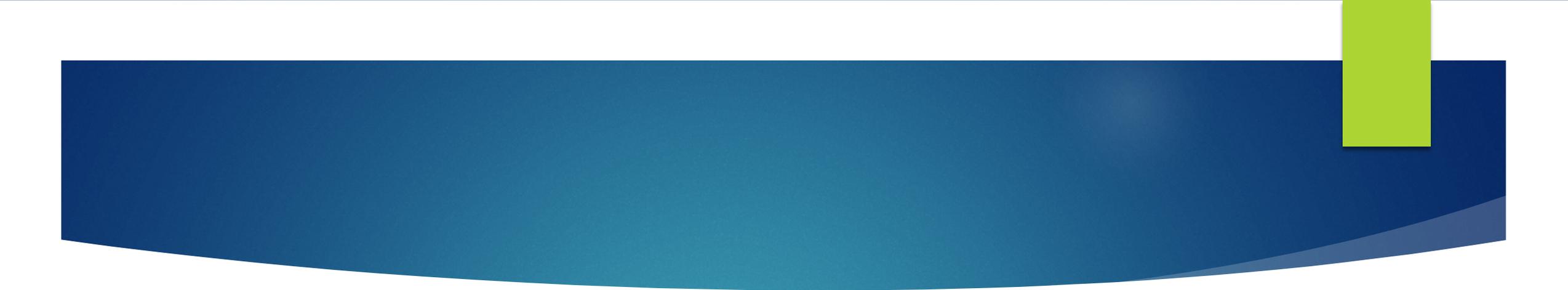




# Security Awareness Training

CJIS SECURITY POLICY V5.4

POLICY AREA 2

- 
- ▶ Level 1: Baseline security awareness training for all authorized personnel with access to CJI.
  - ▶ Level 2: Personnel with both physical and logical access to CJI.
  - ▶ Level 3: Baseline security awareness training for all Information Technology personnel (system administrators, security administrators, and network administrators, etc.).

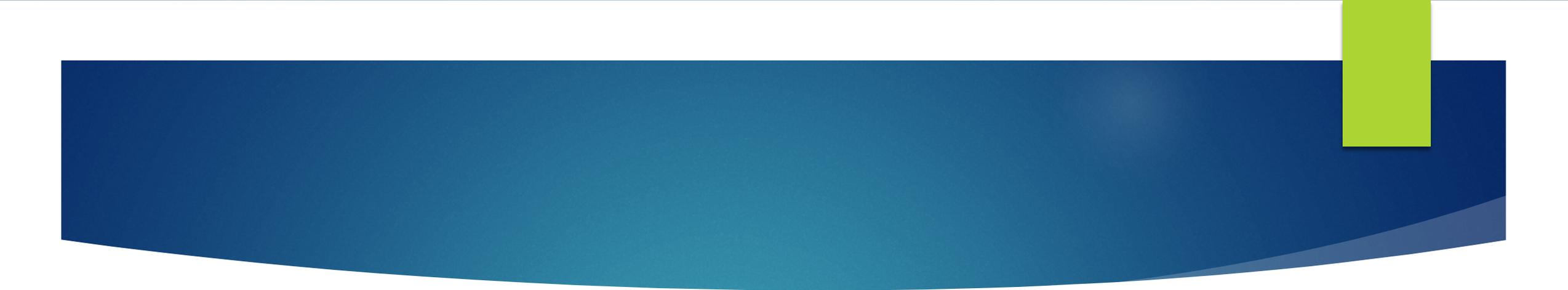


# Level 1

BASELINE SECURITY AWARENESS TRAINING FOR ALL AUTHORIZED  
PERSONNEL WITH ACCESS TO CJJ.

# Level 1 Key Points

- ▶ Rules that describe responsibilities and expected behavior with regard to CJI usage.
- ▶ Implications of noncompliance.
- ▶ Incident response (Points of contact; Individual actions).
- ▶ Media protection.
- ▶ Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity.
- ▶ Protect information subject to confidentiality concerns — hardcopy through destruction.
- ▶ Proper handling and marking of CJI.
- ▶ Threats, vulnerabilities, and risks associated with handling of CJI.
- ▶ Dissemination and destruction.

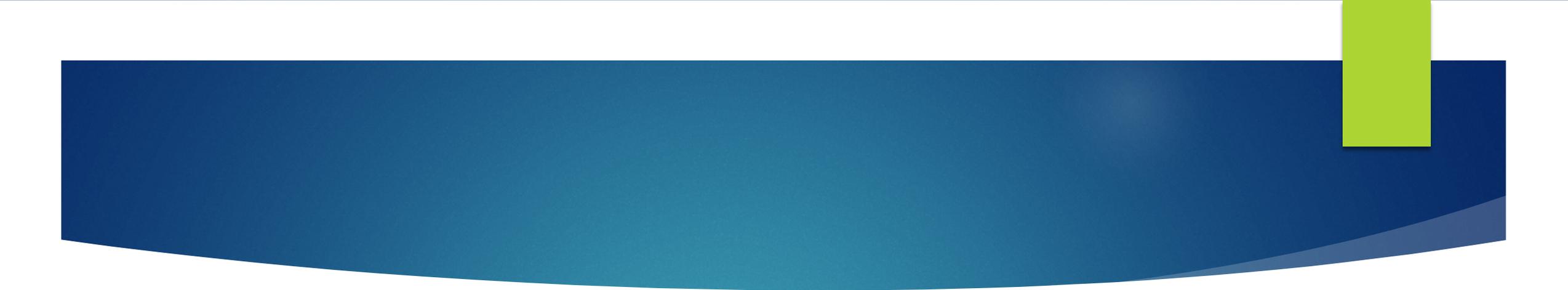


## What

- ▶ The protection of Criminal Justice Information (CJI) originating from the Department of Justice (FBI CJIS data).

## When

- ▶ Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI.



## Who

- ▶ All authorized personnel with access to (physical or logical) CJIS. This includes vendors and anyone who works on and or maintains a technical component that is used to send, receive, process or route a transaction to or from systems that process or maintains FBI CJIS data.

## Why

- ▶ Not only is it required per CJIS Policy, it is each individual's responsibility to protect CJIS with all due diligence. Even the most technically and physically secure environments are subject to threats due to lack of due diligence and or inappropriate conduct from the insider.

## What are we protecting?

Rules that describe responsibilities and expected behavior with regard to CJIS usage.

- ▶ FBI CJIS data is any data derived from the national CJIS Division systems.
- ▶ Many state CJIS systems (they include state hot file and criminal history data) contain FBI CJIS data and must be afforded the same security as national systems.
- ▶ Criminal History Record Information (CHRI) is arrest-based data and any derivative information from that record.
  1. Descriptive Data
  2. Sentencing Data
  3. FBI Number
  4. Conviction Status
  5. Incarceration
  6. Probation & Parole Information

The Interstate Identification Index (III) is also, known as "Triple I" provides for the decentralized interstate exchange of Criminal History Record Information (CHRI) and functions as part of the FBI's CJIS Division's Integrated Automated Fingerprint Identification System (IAFIS). All 50 states return automated CCH information to users based on an inquiry and each state may format their record response differently.

## What are we protecting?

Rules that describe responsibilities and expected behavior with regard to CJI usage. (continued)

Under the III, the FBI maintains an index of persons arrested for felonies or serious misdemeanors under state or federal law.

III includes identification data such as the name, birth date, race, sex and FBI/State identification numbers (SIDS) from each state that has information about an individual.

**Information obtained from the III is considered CHRI and sensitive data and should be treated as such.**

**III may only be accessed for an authorized purpose, and may only be used for the purpose for which it was originally accessed.**

**All users are required to provide a reason for all III inquiries.**

A criminal justice agency is defined as the courts, State & federal Inspector General Offices, and a governmental agency or any subunit thereof that performs the administration of criminal justice pursuant to a statute or executive order and that allocates a substantial part of its annual budget to the administration of criminal justice.

## What are we protecting?

Rules that describe responsibilities and expected behavior with regard to CJJ usage. (continued)

**Voice transmission of a criminal history should be limited, and details of a criminal history should only be given over a radio or cell phone when an officer's safety is in danger or the officer determines that there is a danger to the public.**

Most of the files/data obtained from the National Crime Information Center (NCIC) system are considered restricted files.

There are several files that contain CHRI/CCH information and the dissemination of information should be protected as such:

- Gang File
- Known or Appropriately Suspected Terrorist (KST) File
- Convicted Persons on Supervised Release File
- Immigration Violator File
- National Sex Offender Registry File
- Historical Protection Order File
- Identity Theft File

## What are we protecting?

Rules that describe responsibilities and expected behavior with regard to CJI usage. (continued)

Criminal history record information acquired via CJI Systems **is for use by law enforcement and criminal justice agencies for official criminal justice purposes, consistent with purpose for which the information was requested. Each agency is responsible for maintaining a set of current written policies and procedures that include how the misuse of the NCIC and CCH information will be handled. <local agency note these here>**

Administration of criminal justice means performing functions of detection, apprehension, detention, pretrial release, post trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders by governmental agencies. The administration of criminal justice includes criminal identification activities and the collection, processing, storage, and dissemination of criminal justice information by governmental agencies."

An agency may use a facsimile machine to send a criminal history providing both the sending and receiving agencies have an ORI and are authorized to receive criminal history information.

**Unauthorized requests, receipt, release, interception, dissemination or discussion of FBI CJIS Data/CHRI could result in criminal prosecution and/or termination of employment.**

# Implications of Noncompliance

- ▶ **Any access of these systems and or dissemination of information obtained for non-criminal justice purposes are considered a misuse of the system.**
- ▶ Of the misuse cases that are investigated, most will stem from one of the following categories: affairs of the heart, political motivations, monetary gain, or idle curiosity. Many past cases involved an operator trying to “help out a friend” .
- ▶ **Unauthorized request, receipt or release of CJI material can and has resulted in criminal proceedings.**
- ▶ **Improper use of information obtained from any CJI System and/or related applications and devices may be unlawful, violate federal, state and local policies and may result in prosecution.**
- ▶ **<Placeholder for State/Agency input>**

## Protect information subject to confidentiality concerns (hardcopy through destruction).

- ▶ All agencies are required per CJIS Policy to document and implement policy and procedures to ensure that access to electronic and physical media in all forms is restricted to authorized individuals.
- ▶ All agencies shall securely store electronic and physical media within physically secure locations or controlled areas. If physical and personnel restrictions are not feasible then data shall be encrypted per section 5.10.1.2 of the CJIS Policy.
- ▶ Electronic media consists of memory devices such as hard drives (removable and resident) and transportable media (flash drives, back-up tapes, optical disks, memory cards). In addition, security measures must ensure that CJI in physical (printed documents, printed imagery, etc.) form be protected at the same level.
- ▶ While encryption is the most optimum form of protection, other measures such as layered physical security should be implemented and can include tampering proofing, locked cabinets, and secure transport procedures utilizing vetted personnel such as Law Enforcement Officers. Encryption is the only approved method for email traffic (outside the control of the CJA) containing CJI.

## Protect information subject to confidentiality concerns (hardcopy through destruction).

- ▶ When media is no longer required, proper sanitization or destruction must be carried out.
- ▶ Paper media must be destroyed utilizing approved procedures such as shredding or incineration. Destruction of electronic media shall be carried out by approved methodologies such as degaussing or drive destruction involving shredding or other satisfactory means of destruction.
- ▶ Sanitization of physical media is accomplished by using approved wiping software ensuring a minimal of a 3-pass wipe.
- ▶ It is important to note that sanitization may not be possible for hard drives which fail, therefore, they must be physically destroyed. Degaussing devices must be periodically tested to ensure operability.
- ▶ All sanitization and destruction procedures must be witnessed or carried out by authorized personnel.
- ▶ **<Placeholder for State/Agency input> (reference destruction procedures/policy)**

# Visitor Control and Physical Access

- ▶ All employees are subject to the agency physical protection policy to ensure that the security of CJI is maintained.
- ▶ All employees need to remain cognizant of the designated physically secure areas and ensure that all personnel abide by access control points, entrance and exit procedures, visitor control and handling procedures. Employees must ensure that CJI, whether in physical or electronic form, remain in the secured areas unless they have specific authorization and procedures for taking that information out of the physically secure area.
- ▶ Employees are obligated to report violations and/or suspected violations. Furthermore, employees should report areas of sensitive access that may be unsecure such as emergency exit doors which may have been left propped open. Employees need to maintain vigilance in recognizing individuals who may not have appropriate access and may have been left unescorted.
- ▶ **<Placeholder for State/Agency input>**

# Incident Response

- ▶ A security incident is a violation or possible violation of the technical aspects of the CJIS Security Policy that threatens the confidentiality, integrity or availability of state/FBI CJIS data.
- ▶ **Discuss Agency Policy/Procedures here:**
- ▶ How, who and when to contact.
- ▶ What is applicable to the local agency for level 1 training?  
Unsecured areas that are designated controlled areas  
(areas that CJI resides to include communications closets).

# Proper Handling and Marking of CJI

- ▶ CJI can be leaked inadvertently outside the confines of controlled areas when proper handling and marking procedures are not followed.
- ▶ All physical forms of CJI should be clearly marked and labeled ensuring documents are maintained according to policy and procedures. It is highly recommended that documents, at a minimum be clearly labeled. Coversheets designating the sensitive nature of the data and user responsibility in handling that data should also be considered as an appropriate measure.
- ▶ Electronic forms of media can become mishandled rather quickly due to the hidden nature of the data. Optical media and flash drives should be clearly labeled especially given those forms of media that are not protected by encryption. Lastly, when email contains sensitive information, it should be standard practice to label those items as well and to ensure transmission is encrypted when applicable.
- ▶ **<Placeholder for State/Agency input>**



# Level 2

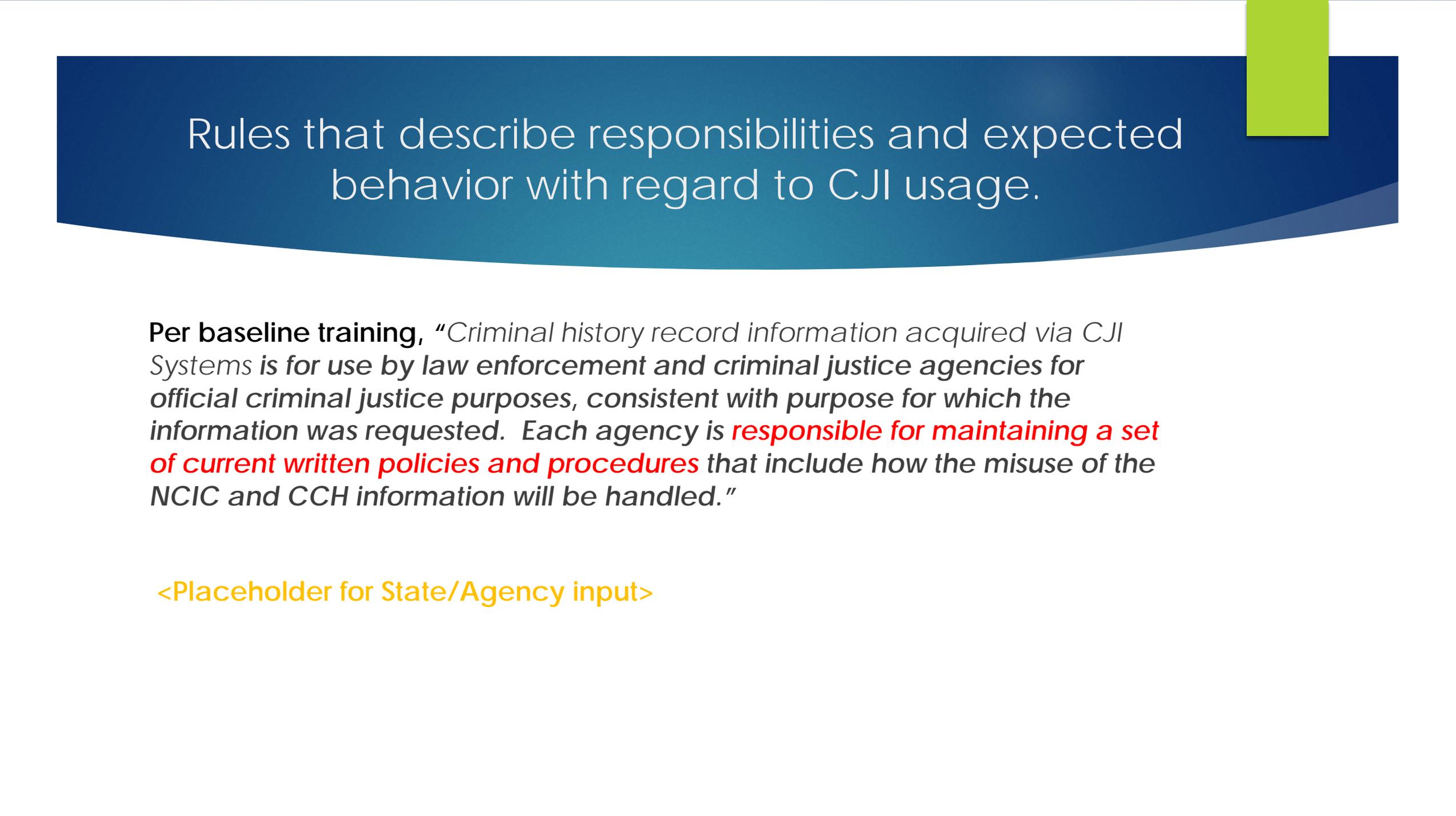
PERSONNEL WITH BOTH PHYSICAL AND LOGICAL ACCESS TO CJI.

# Level 2 Key Points

- ▶ Rules that describe responsibilities and expected behavior with regard to information system usage.
- ▶ Password usage and management—including creation, frequency of changes, and protection.
- ▶ Protection from viruses, worms, Trojan horses, and other malicious code.
- ▶ Unknown e-mail/attachments.
- ▶ Web usage—allowed versus prohibited; monitoring of user activity.
- ▶ Social engineering.
- ▶ Handheld device security issues—address both physical and wireless security issues.
- ▶ Use of encryption and the transmission of sensitive/confidential information over the Internet—address agency policy, procedures, and technical contact for assistance.

## Level 2 Key Points (continued)

- ▶ Laptop security—address both physical and information security issues.
- ▶ Personally owned equipment and software—state whether allowed or not (e.g., copyrights).
- ▶ Access control issues—address least privilege and separation of duties.
- ▶ Physical Security—increases in risks to systems and data.
- ▶ Media Protection.
- ▶ Individual accountability—explain what this means in the agency.
- ▶ Use of acknowledgement statements—passwords, access to systems and data, personal use and gain.
- ▶ Desktop security—discuss use of screensavers, restricting visitors' view of information on screen (mitigating "shoulder surfing"), battery backup devices, allowed access to systems.
- ▶ Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed.
- ▶ Threats, vulnerabilities, and risks associated with accessing CJIS Service systems and services.



Rules that describe responsibilities and expected behavior with regard to CJI usage.

**Per baseline training,** *“Criminal history record information acquired via CJI Systems is for use by law enforcement and criminal justice agencies for official criminal justice purposes, consistent with purpose for which the information was requested. Each agency is **responsible for maintaining a set of current written policies and procedures** that include how the misuse of the NCIC and CCH information will be handled.”*

<Placeholder for State/Agency input>

# Password usage and management—including creation, frequency of changes and protection.

**Password usage shall, at the very least, conform to CJIS policy which currently states the following:**

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 ninety (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.
- CJIS Policy Section 5.6.2.1: Standard Authentication (Password)
  - Users will protect their passwords accordingly, not sharing their individual account access or allowing for the possibility of compromise.

# Protection from Viruses, Worms, Trojan Horses and Other Malicious Code, Unknown E-mail/Attachments.

Per NIST Special Publication 800-83 Revision 1 (Draft) :

“Malware, also known as malicious code, refers to a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim’s data, applications, or operating system. Malware is the most common external threat to most hosts, causing widespread damage and disruption and necessitating extensive recovery efforts within most organizations. Organizations also face similar threats from a few forms of non-malware threats that are often associated with malware. One of these forms that has become commonplace is phishing, which is using deceptive computer-based means to trick individuals into disclosing sensitive information.”

# Protection from Viruses, Worms, Trojan Horses and Other Malicious Code, Unknown E-mail/Attachments.

**Viruses.** A virus self-replicates by inserting copies of itself into host programs or data files. Viruses are often triggered through user interaction, such as opening a file or running a program. Viruses can be divided into the following two subcategories:

- Compiled Viruses. A compiled virus is executed by an operating system. Types of compiled viruses include file infector viruses, which attach themselves to executable programs; boot sector viruses, which infect the master boot records of hard drives or the boot sectors of removable media; and multipartite viruses, which combine the characteristics of file infector and boot sector viruses.
- Interpreted Viruses. Interpreted viruses are executed by an application. Within this subcategory, macro viruses take advantage of the capabilities of applications' macro programming language to infect application documents and document templates, while scripting viruses infect scripts that are understood by scripting languages processed by services on the OS.

**Worms.** A worm is a self-replicating, self-contained program that usually executes itself without user intervention. Worms are divided into two categories:

- Network Service Worms. A network service worm takes advantage of a vulnerability in a network service to propagate itself and infect other hosts.
- Mass Mailing Worms. A mass mailing worm is similar to an email-borne virus but is self-contained, rather than infecting an existing file.

# Protection from Viruses, Worms, Trojan Horses and Other Malicious Code, Unknown E-mail/Attachments.

**Trojan Horses.** A Trojan horse is a self-contained, non-replicating program that, while appearing to be benign, actually has a hidden malicious purpose. Trojan horses either replace existing files with malicious versions or add new malicious files to hosts. They often deliver other attacker tools to hosts.

**Malicious Mobile Code.** Malicious mobile code is software with malicious intent that is transmitted from a remote host to a local host and then executed on the local host, typically without the user's explicit instruction. Popular languages for malicious mobile code include Java, ActiveX, JavaScript, and VBScript.

**Blended Attacks.** A blended attack uses multiple infection or transmission methods. For example, a blended attack could combine the propagation methods of viruses and worms.

# Protection from Viruses, Worms, Trojan Horses and Other Malicious Code, Unknown E-mail/Attachments.

- All users should remain cognizant that their workstations and portable devices are actively being protected with Antivirus/Malicious Code Protection software (per the implementation of the IT staff and local policy and procedures). While this can be mainly automated (via auto update features) for internal systems, end-users play a crucial part in validating that AV definitions remain current on their systems. Of particular interest are portable devices which may have challenges in being updated.
- In addition, end-users play a vital role in following safe practices. Safe practices consist of ensuring any removable devices (CDs, DVDs, Flash Drives) are scanned for virus/malware before introduction to the users system. Users should not download unauthorized content and especially not permit the installation of any software on their systems unless directed by IT staff. Web-based pop-ups should be carefully scrutinized and reported before clicking those windows which may introduce malware. Emails should be screened very carefully and reported if necessary for unsolicited attachments or other embedded objects. Official email and web usage should only be conducted in accordance with official duties so as to limit system interaction with untrusted web sites.

# Web Usage - Allowed versus Prohibited; Monitoring of User Activity; SPAM, Social Engineering

- **Users should consult local policy and/or consult their chain of command for guidance on web usage rules. Users should understand that monitoring of systems and subsequent user activities may be monitored and if necessary investigated .**
- **SPAM is unsolicited email traffic which often times occurs due to the unofficial use of email, forwarding of unofficial email, subscribing to mailing lists, and the leak of official email address to those parties responsible for SPAM.**
- **Social Engineering is the art of manipulating people into performing actions or divulging confidential information. Social Engineering can be accomplished **via Pretexting**: the act of creating and using an invented scenario (the pretext) to engage a targeted victim in a manner that increases the chance the victim will divulge information or perform actions that would be unlikely in ordinary circumstances... or **via Phishing**: e-mail that appears to come from a legitimate business—a bank, or credit card company—requesting "verification" of information and warning of some dire consequence if it is not provided. The e-mail usually contains a link to a fraudulent web page that seems legitimate—with company logos and content—and has a form requesting everything from a home address to an ATM card's PIN. Phishing can also be facilitate over the phone and Interactive Voice Response.**

# Physical Security ~ Increases in Risks to Systems and Data

- ▶ Physical Security basically involves the necessary implementations and methods to enforce access control to secure areas where CJI is processed, stored and transmitted. Since no one agency is the same, local policy and procedures are established to ensure that the established security boundaries are not compromised. This includes not only threats from outsiders but insiders as well.
- ▶ *CJIS Policy addresses key areas such as:*
  - ▶ 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. Terminal areas, Communications Closets/Rooms, Unencrypted communication lines, physical records, etc.
  - ▶ 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.

# Physical Security ~ Increases in Risks to Systems and Data (continued)

## ▶ 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 personal 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.

▶ <Placeholder for State/Agency input>

# Media Protection

Per CJIS Policy, "Media protection policy and procedures shall be documented and implemented to ensure that access to electronic and physical media in all forms is restricted to authorized individuals. Procedures shall be defined for securely handling, transporting and storing media." All personnel should be trained and familiar with local policy and procedures.

- **Media Storage and Access:** shall securely store electronic and physical media within physically secure locations or controlled areas. The agency shall restrict access to electronic and physical media to authorized individuals. (exceptions can be made for encrypted media via consultation with Security Personnel).
- **Media Transport:** shall protect and control electronic and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.
- **Electronic Media in Transit:** "Electronic media" means electronic storage media including 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. Controls shall be in place 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 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 other controls to ensure the security of the data.

# Media Protection

- **Physical Media in Transit:** The controls and security measures also apply to CJJ 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.
- **Electronic Media Sanitization and Disposal:** shall sanitize, that is, overwrite at least three times or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic 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 .
- **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.

# Incident Response

A security incident is a violation or possible violation of the technical aspects of the CJIS Security Policy that threatens the confidentiality, integrity or availability of state/FBI CJIS data.

Users may only see indicators of a security incident. The following is a partial list of incident indicators that deserve special attention from users and/or system administrators:

- The system unexpectedly crashes without clear reasons
- New user accounts are mysteriously created which bypass standard procedures
- Sudden high activity on an account that has had little or no activity for months
- New files with novel or strange names appear
- Accounting discrepancies
- Changes in file lengths or modification dates
- Attempts to write to system files
- Data modification or deletion
- Denial of service
- Unexplained poor system performance
- Anomalies
- Suspicious probes
- Suspicious browsing

# Incident Response (continued)

<Placeholder for State/Agency input>

How, who and when to contact.

What actions to take in case suspected compromise of a terminal for instance (disconnect LAN cable and wait for IT Staff, reporting loss of mobile device, etc.).

# Handheld Device Security Issues ~ Physical and Wireless Security Issues



As electronic handheld devices continue to become more integrated into the mobile workforce, additional measures must be employed since such devices may be used outside of the physical secure locations and may cross nontraditional forms of communication such as commercial wireless and broadband networks.

All agencies are to develop, provide and enforce local policies and procedures that should address areas such as authentication, encryption, security related updates, accountability, official use guidance and incident response measures. These local policies and procedures should be understood by device users.

# Handheld Device Security Issues ~ Physical and Wireless Security Issues (continued)

Factors to consider in developing local policy and procedures are possible loss of the device itself and the technical measures in place to prevent data compromise such as Data at Rest (DAR) encryption. Wireless devices, even in physically secure areas, are susceptible to penetration, eavesdropping and malware. Furthermore, compromised wireless devices may introduce risk to the overall network security of an agency providing unwarranted access.

**<local agency note these here>**

# Personally Owned Equipment and Software

Personally owned equipment and software introduce numerous issues that must be addressed when utilizing that equipment for processing, storing, or transmitting CRI.

- ▶ That equipment shall meet all the requirements set forth in CJIS Policy.
- ▶ Properly licensed hardware and software/Copyright and intellectual property rights.
- ▶ Manageability of those devices by the user's agency: Security and software updates.
- ▶ Threat of data being released into the cloud (lack of control, proper procedures and technical implementation).
- ▶ Devices are not likely to be locked down by a Systems Administrator, due to being a privately owned device, and thus very likely susceptible to penetration, eavesdropping and malware.
- ▶ Sanitization procedures of the device if employee no longer carry out LE duties (whether on good or bad terms).

# Access Control Issues Least Privilege and Separation of Duties

When provided access via an authentication mechanism (login), least privilege, means giving a user account only those privileges which are essential to perform individually assigned duties. The user account is afforded access to information that is strictly on a need to know basis for that individual to perform their duties.

- ▶ While many LE applications restrict access to content based upon an individual's role, many LE applications may not distinguish an individual thus enabling access to information that is not relevant to the duties assigned.

- ▶ While CSAs may control access adequately, local agencies may need to employ additional measures to ensure that individuals do not abuse privileges. Employees should be thoroughly briefed on their particular environment and consent to abide by roles of behavior to prevent unauthorized access to data.

- ▶ Physically secure areas and areas where data resides, electronic or physical, should be protected by access control measures as well.

# Individual Accountability (What Does This Mean to the Agency)

- ▶ Individual's must be held accountable for their actions. CSAs should clearly define standards and roles of behavior for access to CJIS Systems and data. Locals in turn should provide guidance within their own areas of operations and ensure all employees are held accountable for their actions.
- ▶ Individual's must be held accountable for their actions. CSAs should clearly define standards and roles of behavior for access to CJIS Systems and data. Locals in turn should provide guidance within their own areas of operations and ensure all employees are held accountable for their actions.
- ▶ Consequences for breaking agreements should be clearly established and carried out when necessary. Leadership and stakeholders should be in agreement as to the conditions of the agreement and standards of enforcement.
- ▶ **<local agency note these here>**

# Use of Acknowledgement Statements ~ Passwords, Access to Systems and Data, Personal Use and Gain.

- ▶ Acknowledgement statements should be clear, concise, applicable and enforceable. Before being granted access, user should be trained and formally sign an acknowledgement statement for their particular access granted.
- ▶ With access being granted to sensitive information, it is imperative that agencies address the legal ramifications for using that access for personal use and gain.
- ▶ **<local agency note these here>**

# Desktop Security

- ▶ Per the CJIS Policy section on “Session Lock” (5.5.5), “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 officer safety, devices that are: (1) part of a police vehicle; or (2) used to perform dispatch functions and located within a physically secure location, are exempt from this requirement. Note: an example of a session lock is a screen saver with password.
- ▶ Of importance is restricting visitors’ view of information on screen (mitigation of shoulder surfing). Computer screens shall be employed in such a manner so that only authorized individuals are able to view computer screens displaying CJJ.
- ▶ Only authorized and cleared personnel should have access to those systems that process CJJ. Physical access to systems, although logically secure, can be compromised by an insider threat (custodial personnel, maintenance, visitor).
- ▶ Battery backup devices should be employed to prevent loss of data.

# Protect Information Subject to Confidentiality Concerns

Sensitive Information can reside in systems, devices archives, backup media, portable media and hard copy forms. Unless encrypted per CJIS Policy all media shall be stored in a physically secure area under the management control of the CJA. Only those personnel vetted in accordance with CJIS policy may be responsible for protecting information residing in those areas noted above. Upon end of life or other circumstances, media containing sensitive information must be properly sanitized or destroyed according to CJIS Policy and thus in accordance with the method of choice by the local agency.

# Threats, Vulnerabilities, and Risks Associated with Accessing CJIS Systems and Services.

Groups, Individuals, devices, systems and services are increasingly being targeted by both foreign and domestic malefactors based upon association with the Law Enforcement Community. As indicated in previous training, social engineering is one means by which parties may engage an individual in order to carry out illicit activities. Hardware and applications may become compromised therefore personnel operating CJIS Service systems and services require vigilance and need to quickly identify, respond and report incidents per their training.

# Level 3

BASELINE SECURITY AWARENESS TRAINING FOR ALL INFORMATION TECHNOLOGY PERSONNEL (SYSTEM ADMINISTRATORS, SECURITY ADMINISTRATORS, NETWORK ADMINISTRATORS, ETC.)

\* Consult NIST Publications @ <http://csrc.nist.gov/publications/PubsTC.html>

# Level 3 Key Points

- ▶ Protection from viruses, worms, Trojan horses, and other malicious code—scanning, updating definitions.
- ▶ Data backup and storage—centralized or decentralized approach.
- ▶ Timely application of system patches—part of configuration management.
- ▶ Access control measures.
- ▶ Network infrastructure protection measures.

\* Consult NIST Publications @ <http://csrc.nist.gov/publications/PubsTC.html>

# Protection from Viruses, Worms, Trojan Horses, and Other Malicious Code—Scanning, Updating Definitions.

## 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.

### References:

SP 800-83 Rev. 1 DRAFT Guide to Malware Incident Prevention and Handling for Desktops and Laptops

SP 800-124 Rev 1 DRAFT Guidelines for Managing and Securing Mobile Devices in the Enterprise

# Protection from Viruses, Worms, Trojan Horses, and Other Malicious Code—Scanning, Updating Definitions.

## 5.10.4.3 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/or 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 document.

# Protection from Viruses, Worms, Trojan Horses, and Other Malicious Code—Scanning, Updating Definitions.

## 5.13.4.3 Personal Firewall

A personal firewall shall be employed on all devices that are mobile by design (i.e. laptops, handhelds, personal digital assistants, etc.). For the purpose of this policy, a personal firewall is an application that controls network traffic to and from a computer, permitting or denying communications based on policy. 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 PC.
3. Filter incoming traffic by IP address or protocol.
4. Filter incoming traffic by destination ports.
5. Maintain an IP traffic log.

# Protection from Viruses, Worms, Trojan Horses, and Other Malicious Code—Scanning, Updating Definitions.

## 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.

# Protection from Viruses, Worms, Trojan Horses, and Other Malicious Code—Scanning, Updating Definitions.

## **5.10.4.6 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.

# Data Backup and Storage - Centralized or Decentralized Approach.

## 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.

# Data Backup and Storage - Centralized or Decentralized Approach.

## Example:

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 (FIPS 140-2 compliant) Advanced Encryption Standard (AES)-256 bit. 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.

# Timely Application of System Patches - Part of Configuration Management.

## 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.

**\*SP 800-40 Creating a Patch and Vulnerability Management Program**

# Access Control Measures

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.

# Access Control Measures

## 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.

# Access Control Measures (continued)

## 5.5.1 Account Management (continued)

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.

# Access Control Measures (continued)

## 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.

# Access Control Measures (continued)

## **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.

# Access Control Measures (continued)

## 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.

# Access Control Measures (continued)

## 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.

# Access Control Measures (continued)

## 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.

# Access Control Measures (continued)

## 5.5.2.4 Access Control Mechanisms (continued)

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. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is Federal Information Processing Standards (FIPS) 140-2 (as amended) compliant (see section 5.10.1.2 for encryption requirements).
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.

# Access Control Measures (continued)

## **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.

# Access Control Measures (continued)

## 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.

# Access Control Measures (continued)

## 5.5.4 System Use Notification (continued)

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.

# Access Control Measures (continued)

## 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 officer safety, devices that are: (1) part of a police vehicle; or (2) used to perform dispatch functions and located within a physically secure location, are exempt from this requirement. Note: an example of a session lock is a screen saver with password.

# Access Control Measures (continued)

## 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 rationale for such access in the security plan for the information system.

**\*SP 800-12 Guide to General Server Security**

**\*SP 800-11 User's Guide to Securing External Devices for Telework and Remote Access**

# Access Control Measures (continued)

## **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.

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).

# Access Control Measures (continued)

## **5.5.6.2 Publicly Accessible Computers**

Utilizing publicly accessible computers to access, process, store or transmit CJI is prohibited. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

## **5.13. Mobile Devices**

The agency shall: (i) establish usage restrictions and implementation guidance for wireless technologies; 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.

# Access Control Measures (continued)

## 5.13.1 Wireless Communications Technologies

Examples of wireless technologies include, but are not limited to: 802.11x, cellular networks, Bluetooth, satellite and microwave. Wireless technologies require at least the minimum security applied to wired technology and, based upon the specific technology, may require some additional security controls as described below.

### 5.13.1.1 All 802.11x Wireless Protocols

Agencies shall:

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.

# Access Control Measures (continued)

## 5.13.1.1 All 802.11x Wireless Protocols (Continued)

Agencies shall:

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 privacy features.

# Access Control Measures (continued)

## 5.13.1.1 All 802.11x Wireless Protocols (Continued)

Agencies shall:

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 unless the environment is such that the risk has been assessed and is tolerable. Note: some products do not allow disabling this feature; use with caution or use different vendor.
12. Disable all nonessential management protocols on the APs and disable hypertext transfer protocol (HTTP) when not needed or protect HTTP access with authentication and encryption.
13. Enable logging (if supported) and review the logs on a recurring basis per local policy. At a minimum logs shall be reviewed monthly.
14. Segregate, 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.
15. 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.

# Access Control Measures (continued)

## **5.13.3.1 Legacy 802.11 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.

**SP 800-120 Recommendation for EAP Methods Used in Wireless Network Access Authentication**

**SP 800-97 Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i**

**SP 800-127 Guide to Securing WiMAX Wireless Communications**

# Access Control Measures (continued)

## 5.13.1.2 Cellular

Cellular telephones, smartphones (i.e. Blackberry, iPhones, etc.), personal digital assistants (PDA), and “air cards” are examples of cellular handheld devices or devices that employ 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. Cellular devices are at risk due to a multitude of threats and consequently pose a risk to the enterprise.

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 law enforcement officer).
7. Cloning (not as prevalent with later generation cellular technologies).
8. Server-resident data.

# Access Control Measures (continued)

## 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 when an officer determines there is an immediate need for the CJI to further an investigation or situations affecting the safety of an officer or the general public.

# Access Control Measures (continued)

## 5.13.1.3 Bluetooth

Bluetooth is an open standard for short-range radio frequency (RF) communication and is used primarily to establish wireless personal area networks (WPAN), commonly referred to as ad hoc networks or pico nets. A pico net is composed of two or more Bluetooth devices in close physical proximity that operate on the same channel using the same frequency hopping sequence and can scale to include up to seven active slave devices and up to 255 inactive slave devices. Bluetooth voice and data transfer technology has been integrated into many types of business and consumer devices, including cellular phones, personal digital assistants (PDA), laptops, automobiles, printers, and headsets.

Bluetooth does not provide end-to-end, audit, or non-repudiation security services. If such services are needed, they shall be provided through additional, higher-layer means in addition to the Bluetooth specification and 802.11 standards.

The cryptographic algorithms employed by the Bluetooth standard are not FIPS approved. When communications require FIPS-approved cryptographic protection, this can be achieved by employing application-level FIPS-approved encryption over the native Bluetooth encryption.

# Access Control Measures (continued)

## 5.13.1.3 Bluetooth

Agencies shall:

1. Provide users with a list of precautionary measures they should take to better protect handheld Bluetooth devices from theft. The organization and its employees should be responsible for its wireless technology components because theft of those components could lead to malicious activities against the organization's information system resource.
2. Maintain a complete inventory of all Bluetooth-enabled wireless devices and addresses (BD\_ADDRs). A complete inventory of Bluetooth-enabled wireless devices can be referenced when conducting an audit that searches for unauthorized use of wireless technologies.
3. Change the default setting of the Bluetooth device to reflect the organization's security policy. Because default settings are generally not secure, a careful review of those settings should be performed to ensure that they comply with the organization's security policy..
4. Set Bluetooth devices to the lowest necessary and sufficient power level so that transmissions remain within the secure perimeter of the organization. Setting Bluetooth devices to the lowest necessary and sufficient power level ensures a secure range of access to authorized users. The use of Class 1 devices should be avoided due to their extended range (approximately 100 meters).

# Access Control Measures (continued)

## 5.13.1.3 Bluetooth (continued)

Agencies shall:

5. Choose personal identification number (PIN) codes that are sufficiently random and long. Avoid static and weak PINs, such as all zeroes. PIN codes should be random so that they cannot be easily reproduced by malicious users. Longer PIN codes are more resistant to brute force attacks. For Bluetooth v2.0 (or earlier) devices, an eight-character alphanumeric PIN shall be used.
6. For v2.1 devices using Secure Simple Pairing, avoid using the “Just Works” model. The “Just Works” model does not provide protection against man-in-the-middle (MITM) attacks. Devices that only support Just Works should not be procured if similarly qualified devices that support one of the association models (i.e. Numeric Comparison, Out of Band, or Passkey Entry) are available.
7. Bluetooth devices should be configured by default as, and remain, undiscoverable except as needed for pairing. Bluetooth interfaces should be configured as non-discoverable, which prevents visibility to other Bluetooth devices except when discovery is specifically needed. Also, the default self-identifying or discoverable names provided on Bluetooth devices should be changed to anonymous unidentifiable names.
8. Invoke link encryption for all Bluetooth connections regardless of how needless encryption may seem (i.e. no Security Mode 1). Link encryption should be used to secure all data transmissions during a Bluetooth connection; otherwise, transmitted data is vulnerable to eavesdropping.

# Access Control Measures (continued)

## 5.13.1.3 Bluetooth (continued)

Agencies shall:

9. If multi-hop wireless communication is being utilized, ensure that encryption is enable on every link in the communication chain. Every link should be secured because one unsecured link results in compromising the entire communication chain.
10. Ensure device mutual authentication is performed for all accesses. Mutual authentication is required to provide verification that all devices on the network are legitimate.
11. Enable encryption for all broadcast transmission (Encryption Mode 3). Broadcast transmissions secured by link encryption provide a layer of security that protects these transmissions from user interception for malicious purposes.
12. Configure encryption key sizes to the maximum allowable. Using maximum allowable key sizes provides protection from brute force attacks.
13. Establish a “minimum key size” for any negotiation process. Establishing minimum key sizes ensures that all keys are long enough to be resistant to brute force attacks. See Section 5.10.1.2 for minimum key encryption standards.

# Access Control Measures (continued)

## 5.13.1.3 Bluetooth (continued)

Agencies shall:

14. Use Security Mode 3 in order to provide link-level security prior to link establishment.
15. Users do not accept transmissions of any kind from unknown or suspicious devices. These types of transmissions include messages, files, and images. With the increase in the number of Bluetooth enabled devices, it is important that users only establish connections with other trusted devices and only accept content from these trusted devices.

# Access Control Measures (continued)

## Example

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.

# Network Infrastructure Protection Measures

## 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.*

# Network Infrastructure Protection Measures (continued)

## 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 5.10.4.4 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 shall “fail closed” vs. “fail 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.

# Network Infrastructure Protection Measures (continued)

## ► 5.10.1.2 Encryption

1. Encryption shall be a minimum of 128 bit.
2. When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via cryptographic mechanisms (encryption).

EXCEPTIONS: See section 5.10.2.

3. When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected via cryptographic mechanisms (encryption).
4. When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards.

Note 1: 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.

Note 2: While FIPS 197 (Advanced Encryption Standard) certification is desirable, a FIPS 197 certification alone is insufficient as the certification is for the algorithm only vs. the FIPS 140-2 standard which certifies the packaging of an implementation.

# Network Infrastructure Protection Measures (continued)

## 5.10.1.2 Encryption (continued)

5. For agencies using public key infrastructure 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.

**\*SP 800-15 MISPC Minimum Interoperability Specification for PKI Components**

**\*SP 800-96 PIV Card to Reader Interoperability Guidelines**

**\*SP 800-111 Guide to Storage Encryption Technologies for End User Devices**

# Network Infrastructure Protection Measures (continued)

## 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.

**\*SP 800-94 Rev. 1 DRAFT Guide to Intrusion Detection and Prevention Systems (IDPS)**

# Network Infrastructure Protection Measures (continued)

## 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.

# Network Infrastructure Protection Measures (continued)

## 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.

**\*SP 800-125 Guide to Security for Full Virtualization Technologies**

# Network Infrastructure Protection Measures (continued)

## 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.

# Network Infrastructure Protection Measures (continued)

## 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 that process CJI internally.
4. Device drivers that are "critical" shall be contained within a separate guest.

# Network Infrastructure Protection Measures (continued)

## 5.10.3.2 Virtualization (continued)

The following are additional technical security control best practices and should be implemented wherever feasible:

1. Encrypt network traffic between the virtual machine and host.
2. Implement IDS and IPS monitoring within the virtual machine environment.
3. Virtually firewall each virtual machine from each other (or physically firewall each virtual machine from each other with an application layer firewall) and ensure that only allowed protocols will transact.
4. Segregate the administrative duties for the host.

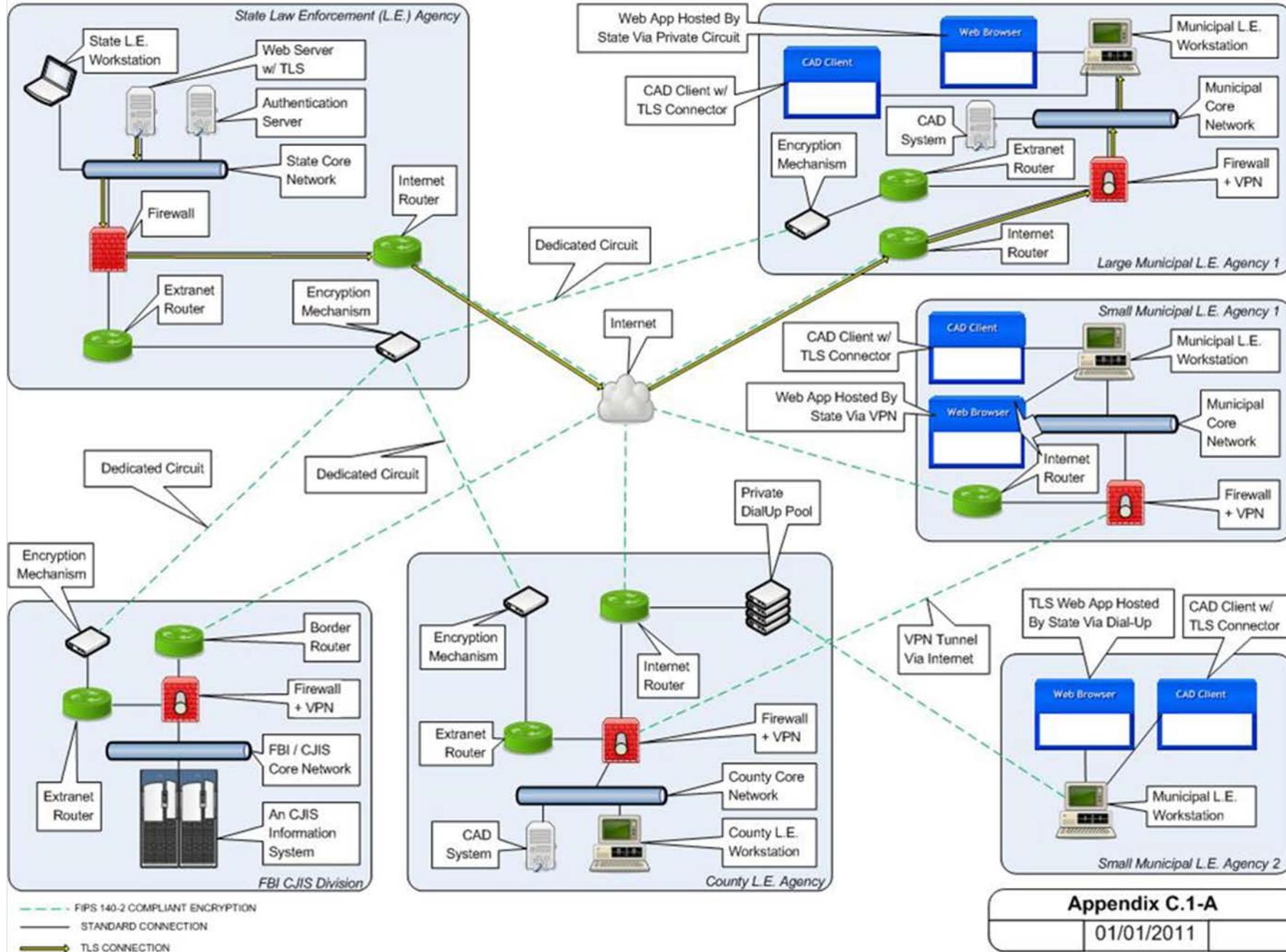
Appendix G of the FBI CJIS 5.4 Policy provides some reference and additional background information on virtualization.

# Network Infrastructure Protection Measures (continued)

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.

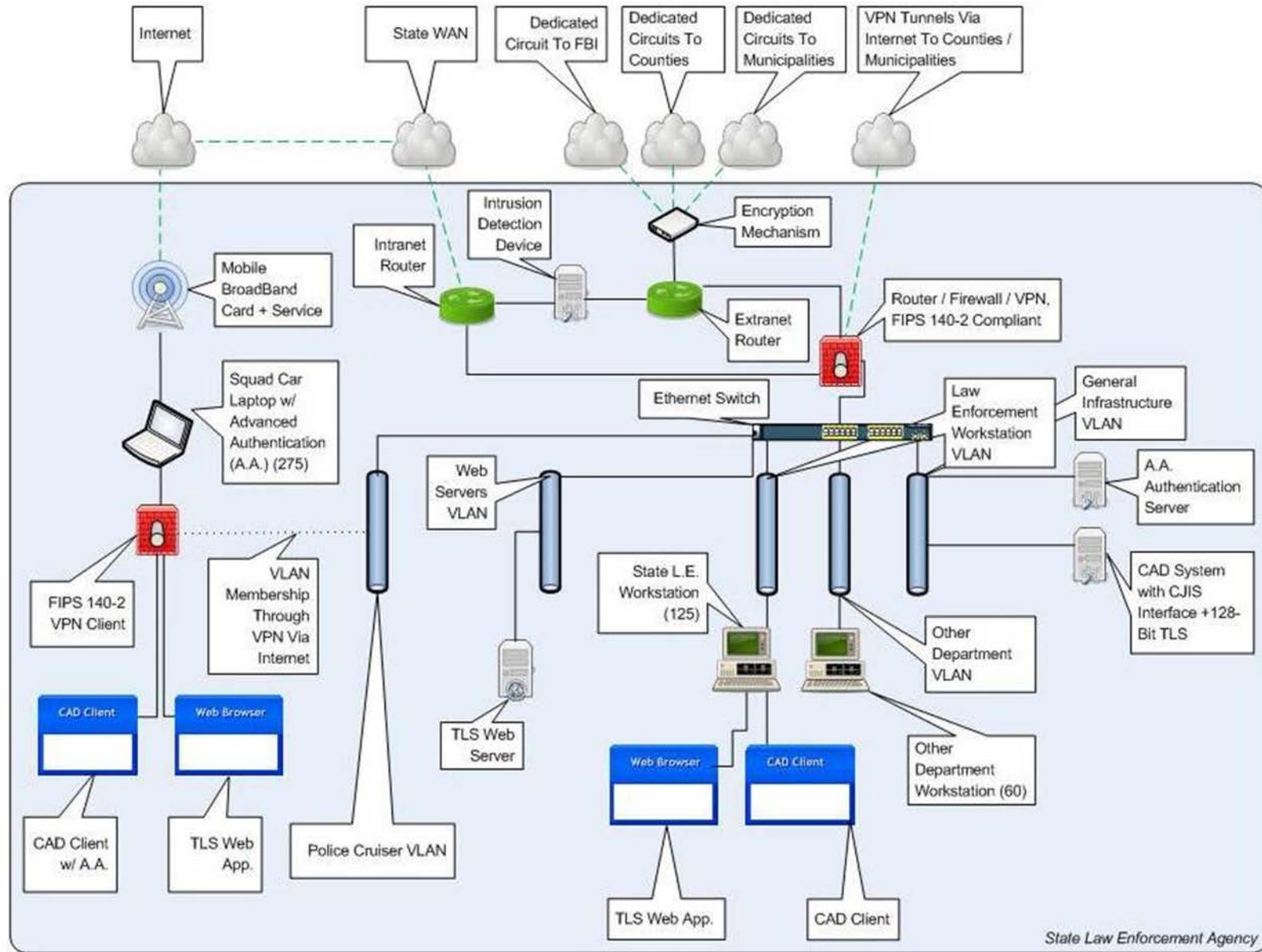
# Overview: Conceptual Connections Between Various Agencies



Appendix C.1-A

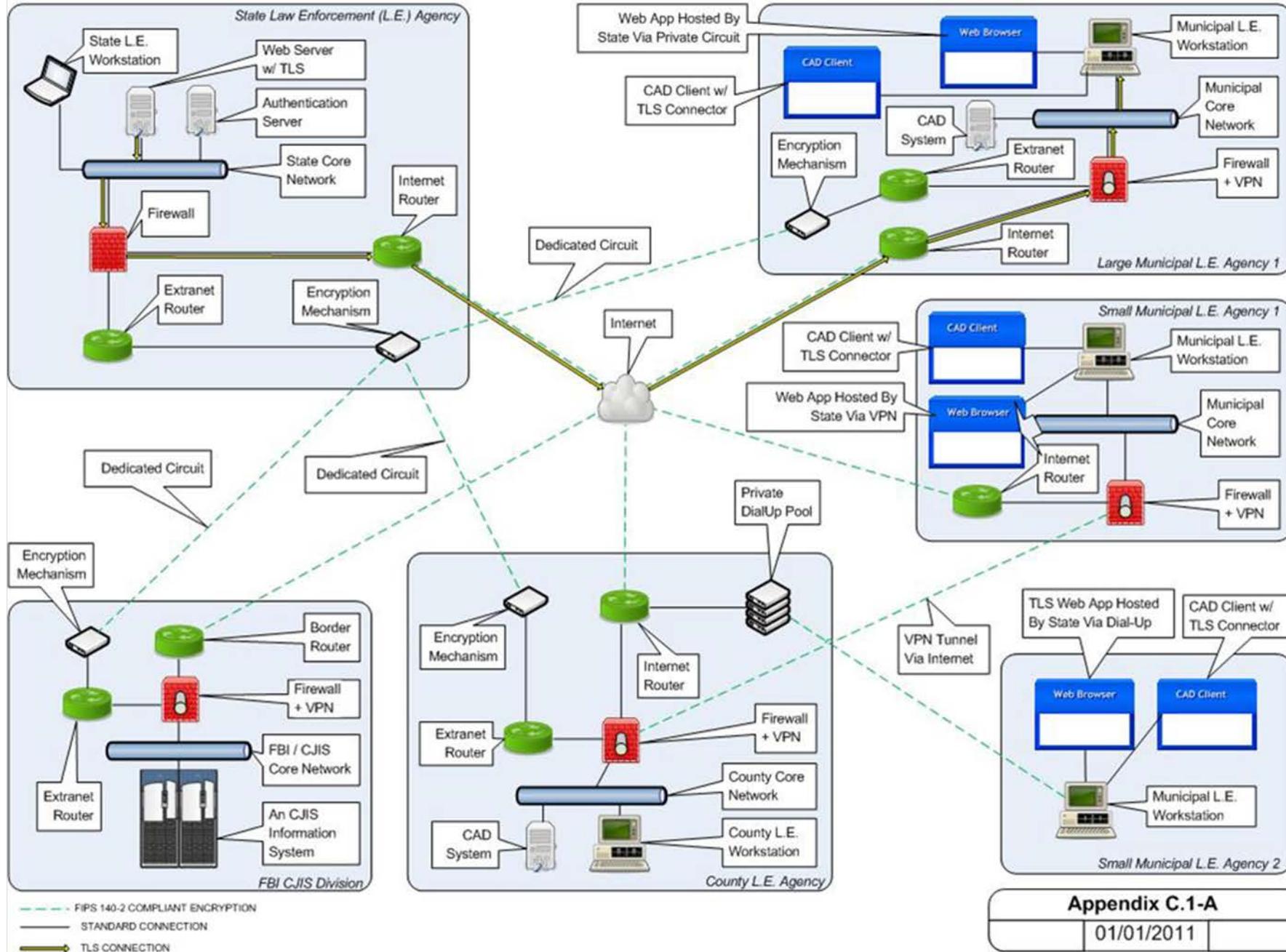
01/01/2011

# Conceptual Topology Diagram For A State Law Enforcement Agency



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

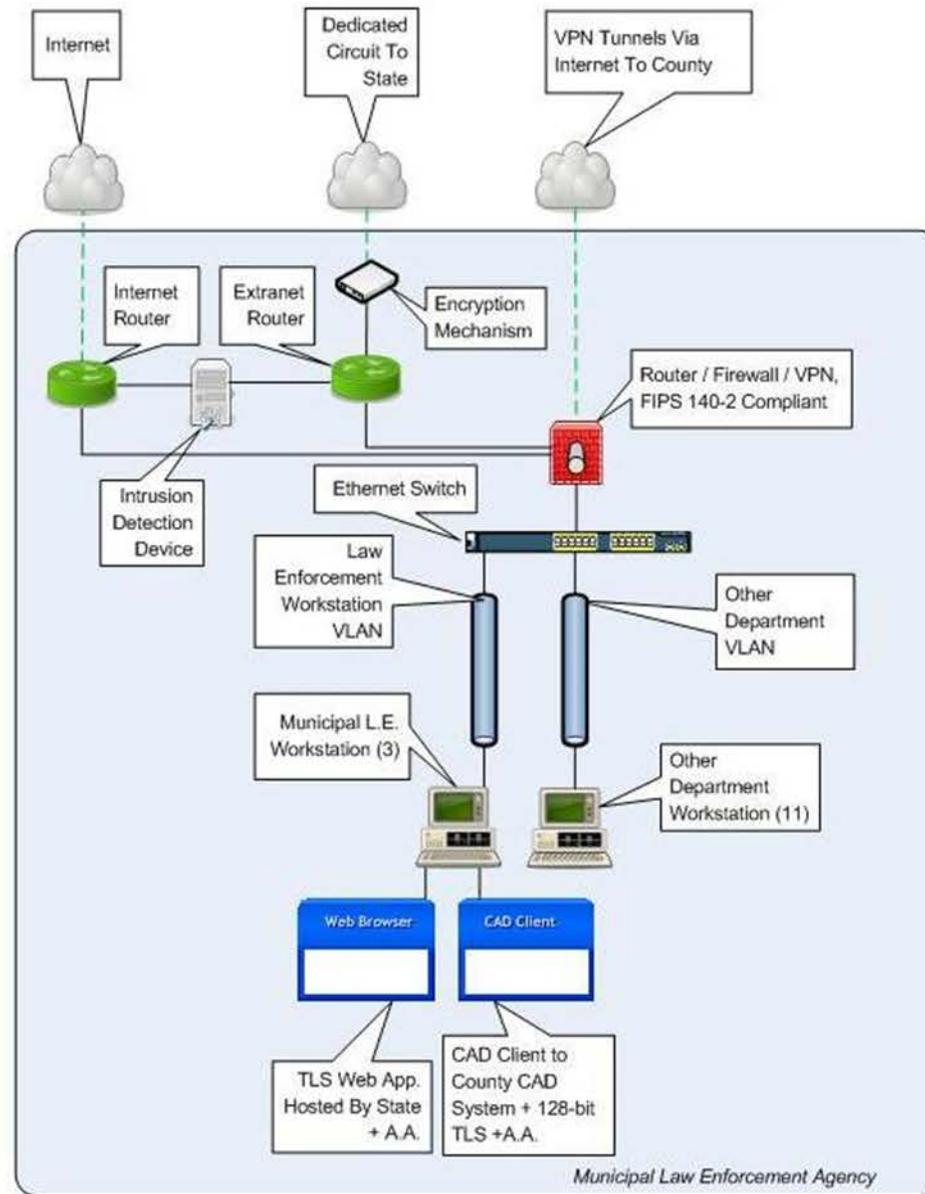
# Overview: Conceptual Connections Between Various Agencies



Appendix C.1-A

01/01/2011

# Conceptual Topology Diagram For A Municipal Law Enforcement Agency



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

|                       |  |
|-----------------------|--|
| <b>Appendix C.1-D</b> |  |
| 01/01/2011            |  |