



# Rap Sheet (Special Edition)

## Review of the CJIS Security Policy 5.0

It seems every day we hear news reports about computer hacking and 'cyber attacks' on computer networks and information services. The Criminal Justice Information Services (CJIS) Systems (managed by the Michigan State Police [MSP] Criminal Justice Information Center [CJIC]) and the National Crime Information Center (NCIC) System (managed by the FBI's Criminal Justice Information Services Division) are computer networks that provide access to sensitive and confidential information. To help keep this information network safe, the FBI's CJIS Division has laid out "ground rules" agencies must follow in order to obtain access to any Criminal Justice Information (CJI). These rules are contained in the FBI CJIS Security Policy. All agencies must minimally comply with the FBI CJIS Security Policy to maintain access to CJI.

The current version of the FBI CJIS Security Policy, version 5.0, was signed into effect in February 2011. The new policy is a complete rewrite. In some cases existing requirements continue, but are found in new locations within the policy. In others, what has been suggested as good business practice is now documented as required policy items. In addition, there are new requirements regarding visitor logs, auditing, agency policy, personally owned devices, training, and more. Some of these requirements must be met immediately, and others do not become effective until 2012 or 2013.

This special edition of the Rap Sheet newsletter is an effort to ensure all agencies are aware of both the current and future security requirements that must be met to maintain system access. The articles in this newsletter provide basic information about an issue/requirement, indicating what items must currently be in place and what is coming in that area in the future. If your agency wishes to view a copy of version 5.0 of the CJIS Security Policy in its entirety, it can be found at [www.michigan.gov/LEIN](http://www.michigan.gov/LEIN).

As the use of technology in the law enforcement world continues to grow and evolve, we all must take steps to protect the networks that provide you with access to the information you need to perform your job each day. Please feel free to contact me or the Information Security Officer (ISO), Terri Smith, to discuss your thoughts and get answers to your questions regarding access to CJIS Systems.

Dawn Brinningstall  
Director, Criminal Justice Information Center  
CJIS Systems Officer

### Inside this issue:

|                             |     |
|-----------------------------|-----|
| Security Awareness Training | 2   |
| Security Incidents          | 2   |
| Internal Accountability     | 2   |
| Systems Access              | 3   |
| Current Requirements        | 4   |
| User IDs & Logins           | 4   |
| User Authentication         | 5   |
| Password Requirements       | 5   |
| Network Configuration       | 6   |
| Media Protection            | 6   |
| Physical Security           | 7   |
| Basic Requirements          | 8   |
| Communications Protection   | 8-9 |
| Authorized Persons          | 9   |
| Discipline                  | 10  |
| Written Policy              | 10  |
| Timetable                   | 11  |

## Security Awareness Training

The CJIS Security Policy requires that Security Awareness Training be completed at least once every two years by all personnel who manage or have access to CJIS/NCIC Systems. Anyone who has access to CJI data/systems must receive security awareness training within six months of gaining access. Security awareness training must be renewed every two years. *This includes* any appropriate information technology (IT) personnel/vendors who maintain network hardware/software, and those who have unescorted access to secure areas (for example cleaning personnel, clerical staff, administrative support staff, etc.). A security awareness training PowerPoint is available on the MSP Web site at [www.michigan.gov/LEIN](http://www.michigan.gov/LEIN).



**Future:** In 2013, security awareness training will also be required for *all* personnel who access or receive criminal justice information from the system. For example, security awareness training would then be required for district attorney staff/prosecutors who receive printouts or files containing system printouts, and for officers at non-terminal agencies your agency dispatches for and provides with CJI printouts.

**Reference:** CJIS Security Policy Section 5.2



## Security Incidents: What Do I Do?

There has been an increase in the number of accidental or malicious computer attacks against both government and private agencies, regardless of whether the systems are high or low profile. Agencies must track and document information system security incidents on an ongoing basis. They must also track, document, and report possible security incidents to the Michigan CJIS Systems Agency (CSA). Please see the reporting form in Appendix F of the CJIS Security Policy.

**Future:** Beginning in 2012, agencies must establish an operational incident handling capability for their information systems that includes adequate preparation, detection, analysis, containment, recovery and user response activities. Also in 2012, wherever feasible the agency must employ automated mechanisms to support the incident handling process.

**Reference:** CJIS Security Policy Section 5.3

## Internal Accountability

An agency's information system must generate records for defined events. Currently, these records must include records of successful/unsuccessful login attempts.



**Future:** Beginning in 2012, these audit/accountability records must be maintained for at least 365 days.

In 2013, new requirements with regards to these audit records, including specifying additional information content that must be captured (such as successful/unsuccessful attempts to change account passwords, and successful/unsuccessful attempts to create, write, delete or change permission on a user account, a file, a directory, or another system resource). The records must also include successful/unsuccessful actions by privileged accounts, and successful/unsuccessful attempts by users to access, modify or destroy the audit log file. The records must also then be reviewed/analyzed at least once a week. The records must be time stamped when generated, and the records must be maintained until they are no longer needed. Agencies must also ensure their system provides alerts to appropriate persons in the event there is a failure in processing audit records.

**Reference:** CJIS Security Policy Section 5.4.7, Section 5.5.3

## System Access



Access to the CJI Systems must be controlled to ensure only authorized users have access, and to reduce the risk of unauthorized activity. Thus, agencies must approve individual access privileges and grant access only if there is a valid need for access as determined by assigned official duties and only if the subject has satisfied all personnel security criteria. When access is granted, agencies must ensure the most restrictive set of rights/privileges is assigned to the user for the performance of specified tasks. When a user's need for access changes or the user is terminated or transferred, the user's account must be removed/disabled/or updated as appropriate.

Agencies can use any one of a number of methods to control system access: access control lists, resource restrictions, encryption, or control access at the application level.

Where technically feasible, an agency must enforce a limit of no more than five consecutive invalid access attempts by a user before automatically locking the account for at least ten minutes (unless the account is released by an administrator). Also, if a session is inactive for a maximum of 30 minutes, the agency must initiate a session lock that remains in effect until the user re-establishes access using appropriate identification and authentication

procedures. Devices that are part of a police vehicle or used to perform dispatch functions and located in a physically secure location are exempt from this requirement. Note: an example of a session lock is a screen saver with password.

**Using publicly accessible computers to access, process, store or transmit criminal justice information is prohibited.** Examples of publicly accessible computers include (but are not limited to) hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

**Future:** In 2012 numerous additional restrictions go into effect for wireless access. Please see the CJIS Security Policy for details. Also, beginning in 2012, agencies must validate all user accounts at least annually and must document the validation process.

By 2013, agencies must have access control policies in place. Users must directly initiate a session lock mechanism to prevent inadvertent viewing when a device is unattended. Beginning in 2013, systems must display a system use notification message on screen that users must acknowledge before logging in. The message must advise the user that they are accessing a restricted system, that system usage may be monitored, recorded, and subject to audit, that unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties, and that use of the system indicates consent to monitoring and recording. Beginning in 2013, any remote access to the information system must be authorized, monitored, and controlled by the agency. Remote access is any temporary access to an agency's information system communicating temporarily through an external non-agency-controlled network, i.e. the Internet. Remote access must be controlled through managed access points, and an agency must employ automated mechanisms to aid in the monitoring and control of remote access methods.

**Reference:** CJIS Security Policy Section 5.5

## You Should Already Be Doing This

CJI users, especially agency TACs and information services personnel, should be aware a key deadline has passed regarding the FBI's CJIS Security Policy. Agencies should already have implemented the requirements below. September 30, 2010 was the deadline for agencies connected to/accessing NCIC to come into compliance with the following policy requirements:



In addition, changes to the CJIS Security Policy in 2010 changed the requirement for security awareness training from every 3 years to every 2 years. The following additional requirements were also put in place:

- Least privilege – agencies must enforce the most restrictive set of rights/privileges or access needed by users for the performance of assigned tasks.

**Reference:** CJIS Security Policy Section 5.5.2.1

- Login attempts – Where technically feasible, agencies must enforce a limit of no more than five consecutive invalid access attempts by a user before their account is locked for a minimum of ten minutes.

**Reference:** CJIS Security Policy Section 5.5.3

- Session locks – after a maximum of 30 minutes of inactivity on a terminal, the agency/software must initiate a session lock. The terminal must remain locked until the user re-establishes access using the appropriate identification and authentication (i.e. userid/password). *Devices within a police vehicle or used to conduct dispatch functions within a physically secure location are exempt from this requirement.*

**Reference:** CJIS Security Policy Section 5.5.5

## User IDs and Logins

Anyone accessing the CJI Systems must be uniquely identified/have their own unique login. This includes IT personnel/vendors who maintain the system or network. Before being allowed to perform any actions on the system, users must use this unique ID to identify themselves. Agencies must make sure all user IDs belong to current authorized users, and keep this information current by adding new user IDs and deleting and/or disabling former user's IDs.



**Future:** Beginning in 2012, agencies must document their process for establishing/issuing user IDs, including how each user is uniquely identified, how their identity is verified, who is authorized to issue new user IDs and how a request for user IDs is received. Agencies will need to document how the user ID is issued to the user, how IDs are disabled after a specified period of inactivity, and how user IDs are archived.

**Reference:** CJIS Security Policy Section 5.6

## User Authentication: Standard/Advanced

A CJI user ID uniquely identifies the subject, but a second step is needed to authenticate the user is who they say they are. Each user's identity must be authenticated.

The simplest, standard way of authenticating a user is by use of a password. Password requirements are outlined in a separate article in this newsletter. (See page 5)

Some types of system access require Advanced Authentication for additional security. Forms of Advanced Authentication may include biometric systems, user based public key infrastructure (PKI), smart cards, software tokens, hardware tokens, paper tokens, or risk based authentication.

Whether or not Advanced Authentication is needed depends on the physical, personnel and technical security controls associated with the user location. For example, agencies transmitting CJI data using wireless methods or via the Internet must employ an accepted form of Advanced Authentication.

Agencies currently using a VPN with IPSec to meet the Advanced Authentication requirement from a police vehicle may continue to do so until 2013. Such agencies will want to begin to investigate another authorized method of Advanced Authentication.

**Future:** Beginning in 2012, agencies must have written policy detailing their authentication strategy. Agencies must document their process for managing authenticators, including defining initial authenticator content, establishing administrative procedures for initially distributing authenticators, establishing procedures for how lost/compromised or damaged authenticators are dealt with and for how authenticators are revoked. Agencies will also need to document how default authenticators are changed upon information system installation, and how authenticators are changed or refreshed periodically.

**Reference:** CJIS Security Policy Section 5.6

## Password Requirements

For access to CJI, secure passwords must be used. Agencies should have already implemented the requirements below:

- Passwords must be at least eight characters in length.
- User cannot reuse their last ten passwords.
- Passwords cannot be transmitted in the clear.
- Passwords cannot be a dictionary word or proper name or match the userid.
- Passwords must be changed at least every 90 days.
- All workstations with wireless access must have an activated personal or software based firewall.
- Wireless or dial-up access must use an approved form of Advanced Authentication. (See page 8)
- Any data transmitted over a public segment, by dial-up, using wireless or via the Internet must be encrypted at a minimum of 128 bit **and** meet the FIPS 140-2 NIST certification standard.

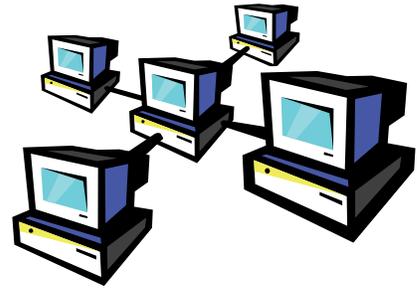
**Reference:** CJIS Security Policy Section 5.6.2.1

These changes also clarified that VPNs currently used for Advanced Authentication from a police vehicle will be allowed until 2013 if the VPN uses IPSec. If you have questions regarding these important deadlines and changes to security requirements, contact Ms. Terri Smith, ISO at [SmithTA@michigan.gov](mailto:SmithTA@michigan.gov).



## Network Configuration

Any changes to an agency's computer network may affect the security of the system. An agency must maintain a current topological drawing depicting the agency's computer network and its connection to the CJIS Systems, and this drawing must be available for review during a LEIN audit. The diagram must show all communication paths, circuits and components used to connect to the CJIS Systems, beginning at the agency and traversing through all interconnected systems. The diagram must show the logical location of all components (firewalls, routers, switches, etc.). Each individual workstation/client need not be shown; the number of clients is sufficient. Mark on the diagram the agency name, date of creation, and indicate that the diagram is "For Official Use Only."



Only authorized persons are allowed to have access to the system components to make changes, upgrades, and modifications. The agency must configure the application used to access the system to provide each person with only the essential capabilities and must restrict the use of certain functions.

**Reference:** CJIS Security Policy Section 5.7

## Media Protection

CJIS data may be present on various forms of electronic media. Laptops used as mobile data terminals may contain residual CJIS information. Desk top hard drives may contain leftover information, or users may have transferred CJIS information to disc, CDs, or flash drives. CJIS data, whether contained on some form of electronic media or in the form of a paper print-out, must be stored, transported, and disposed of in a secure manner.

CJIS System data, whether stored on electronic media or stored in the form of physical print-outs, must be stored in a physically secure location. Access to the physically secure location must be restricted to authorized individuals. Authorized individuals are those who successfully completed the required fingerprint based background check and received security awareness training.



Many times criminal justice information obtained from the CJIS Systems must be physically moved from one location to another. Once again, whether the data is an electronic or paper form, the data must be protected while in transit to prevent compromise of the data. An agency must have controls in place to protect CJIS data while in transit.

When the data is no longer needed, it must be disposed of in a secure manner. For physical media such as printouts, this means disposal by cross-shredding or incineration. For electronic media, this means degaussing or sanitizing the media (overwriting at least three times) or if the media is inoperable it must be destroyed, shredded, cut-up, etc.). There must be formal written policy on disposal procedures/methods, and the agency must maintain written documentation of the steps taken to sanitize or destroy electronic media.

Disposal, destruction or sanitization of media, whether electronic or physical paper, must either be carried out by authorized personnel (those who have completed the required fingerprint-based background check and received security awareness training) or the destruction must be witnessed by authorized personnel.

**Reference:** CJIS Security Policy Section 5.8

## What is Physical Security?



As you know, computers that access CJJ must be placed in a physically secure location to protect hardware, software and media. This would include workstations within your physically secure location. So what exactly is a physically secure location? According to the FBI, it is a criminal justice facility, area, room, group of rooms within a criminal justice agency, or that are under the control of a criminal justice agency through a signed management control agreement, an FBI CJIS security addendum or a combination of both.

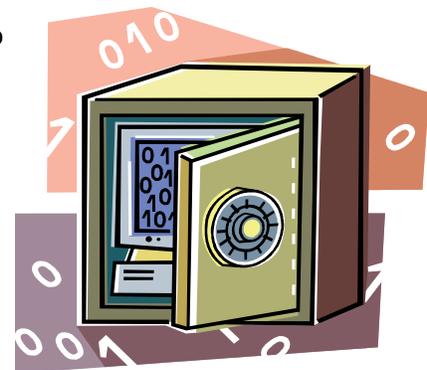
Computers with CJJ access in police vehicles must be protected with additional security such as Advanced Authentication and FIPS 140-2 compliant encryption. A police vehicle is defined as an *enclosed* criminal justice conveyance. So while a squad car would meet this definition, a patrol motorcycle would not. Restricted areas must be prominently posted and separated from non-restricted areas by physical barriers that restrict unauthorized access. Computer monitors/displays must be positioned so the public/other unauthorized persons cannot view system information. Any access point to the restricted areas must be controlled or secured during both working and nonworking hours, and an agency must verify an individual's access authorization before granting them access to a secure area. Do not just assume because someone is in uniform they are authorized to access the secure area. Visitors to the secure areas must be escorted at all times, and visitors must be authenticated before escorting them in the secure areas.

So who is a visitor? If the person is requesting unescorted access and has not completed the required background check and received security awareness training (See page 10), they are considered a visitor. If your agency wants to grant them unescorted access to your secure location, the required background check and security awareness training must be completed and your agency must add them to your authorized access list. It is important to monitor access to secure areas to detect and respond to physical security incidents.

**Future:** New requirements with regards to physical security are applicable in 2012. In 2012, agencies must keep records detailing visitor access to the secure location, and these records must be maintained at least one year. These visitor access records must include the name and agency of the visitor, their signature, what form of identification was used to identify the visitor, date of access, time of entry and departure, purpose of their visit and name and agency of who they visited.

Beginning in 2013, an agency must keep a current list of personnel who are authorized to have access to the secure area. Also beginning in 2013, agencies must monitor delivery and removal of equipment and transmission lines used to access the system.

**Reference:** CJIS Security Policy Section 5.9



## Basic Requirements

Agencies attempting to comply with CJIS Security Policy often say “Just tell me what to do. Here is the type of computer network I have, tell me what I have to do and I’ll do it.”

Unfortunately, it is not that easy....

The CSA, CJIS Systems Officer (CSO), or ISO cannot endorse specific products or software. Each agency must find the solution that meets their unique needs and the needs of their particular network. But keep these basic requirements in mind:



**Wireless:** If your agency transmits CJI data over a wireless network (such as MDCs) each device with wireless access must have an activated personal or software based firewall. CJI data must be encrypted at a minimum of 128 bit and the encryption used must meet the FIPS 140-2 standard. Wireless access must also use an approved form of Advanced Authentication.

**Internet:** If your agency transmits CJI data over the internet, CJI data must be encrypted at a minimum of 128 bit and the encryption used must meet the FIPS 140-2 standard. Internet access must also use an approved form of Advanced Authentication.

**Public Segment:** As mentioned before, access to the CJIS & NCIC Systems and the information they contain is restricted to law enforcement/criminal justice agencies. As such, CJI data must be protected any time it is possibly open to public view.

*Outside your agency’s secure area:* If your agency transmits CJI data over a public network segment (such as a T1 line owned by AT&T, etc.) the CJI data must be encrypted at a minimum of 128 bit and the encryption used must meet the FIPS 140-2 standard.

*Within your agency’s physically secure area:* Your agency may share part of its computer network with another public agency such as a fire department, parks department, etc. Any CJI data transmitted over this shared network either must be encrypted at a minimum of 128 bit and the encryption used must meet the FIPS 140-2 standard or there must be a physical separation of CJI data from other data transmitted over the network (separate virtual local area networks [VLANs], etc.). VLANs should be protected/secured with access control lists to logically separate the traffic.

**Reference:** CJIS Security Policy Section 5.9.1

## Communications Protection: Flow, Viruses and Spam



Agencies must control the flow of information between interconnected systems. Information flow control regulates where information is allowed to travel within a system and between systems.

Agencies must also implement virus protection mechanisms to detect and eradicate malicious code at critical points throughout their network and on all workstations, servers and mobile computing devices on the network. Malicious code protection must be enabled and resident scanning must be employed.

Any device that is mobile by design (laptops, handhelds, personal digital assistants, etc.), must employ a personal/software firewall that manages program access to the Internet, blocks unsolicited requests to connect to the PC, filters incoming traffic by IP address, protocol, or destination port, and maintains an IP traffic log.

**Future:** Agencies should be aware that specific requirements for the use of partitioning and virtualization become effective in 2012. By 2012, agencies must begin regularly receiving system security alerts, take appropriate action, and document the type of action taken.

Agencies are also required by 2012 to implement malicious code protection that includes automatic updates for all systems with Internet access. If an agency system is not connected to the Internet, they must implement local procedures to ensure malicious code protection is kept current. Agencies must implement spam protection at critical information system entry points, and must employ spyware protection at workstations, servers, or mobile computing devices on the network. The spam and spyware protection must be used to detect and take appropriate action on unsolicited messages and spyware/adware transported by e-mail, e-mail attachments, Internet access, or removable media.

Additional requirements must be met in 2012 and 2013 for boundary protection monitoring, network and/or host based intrusion detection tools, and additional requirements for the encryption of information is stored electronically outside the boundary of the physically secure location.

**Reference:** CJIS Security Policy Section 5.10

## Authorized Persons



The FBI CJIS Security Policy requires state and national criminal history record checks be conducted within 30 days of initial employment or access for all personnel who will have physical or logical access to systems, unencrypted system data, or have the direct responsibility to configure and maintain systems and network with direct access to Michigan and FBI CJIS Systems.

Below is a non-inclusive list of individuals with unescorted access requiring a background clearance:

- Dispatch personnel
- IT personnel, contractors or vendors
- Janitorial personnel
- Clerical or administrative personnel

The minimum check must include submission of completed applicant fingerprint cards to the FBI CJIS Division and the MSP. The Michigan and NCIC Wanted Person Files must also be checked. The good news is sworn personnel who have been fingerprinted and certified by the Michigan Commission on Law Enforcement Standards (MCOLES) already meet this requirement. When fingerprint identification of an applicant/employee has been established and he/she appears to be a wanted person or to have an arrest history for a felony or serious misdemeanor, the employing agency *must* delay granting NCIC access until the matter is reviewed to determine if system access is appropriate.

If a felony conviction of any kind exists, the agency shall deny systems access. However, the hiring authority may ask for a review by the CJIS Systems Officer (CSO) at the MSP in extenuating circumstances (where the severity of the offense and the time that has passed would support a possible variance). Other offenses may be disqualifying at the discretion of the agency. Background reinvestigations are recommended every five years as a good business practice. If the person already has access to CJIS Systems and is subsequently arrested and or convicted, continued access to CJIS shall be determined by the CSO.

**Reference:** CJIS Security Policy Section 5.12



## Discipline

Agencies must have a written policy/formal sanctions process for personnel who fail to follow CJIS system policies, including information security policy and procedures.

**Reference:** CJIS Security Policy Section 5.12.4

## Written Policy

How many times have you heard “If it’s not on paper, it didn’t happen”? Documentation is an integral part of the law enforcement/criminal justice field, and the CJIS Security policy requires agencies to have written policies in place dealing with several situations. So what needs to be in your policy manual?



**Possible Security Incidents/Events:** Formal information security event reporting and escalation procedures must be in place. All employees/contractors/third party users must be made aware of the procedures for reporting the different types of events and weaknesses that might have an impact on the security of agency assets and are required to report any information security events and weaknesses as quickly as possible to the designated point of contact (CJIS Security Policy Section 5.3.1, effective 2012).

**Access Control:** Access control policies must be employed to control access between users and objects in the information system (CJIS Security Policy Section 5.5.2, effective 2013).

**Managing Authenticators:** The agency must manage authenticators (tokens, user-based PKI certificates, etc.) by establishing administrative procedures for initial authenticator distribution, lost/compromised/damaged authenticators, and revoking authenticators (CJIS Security Policy Section 5.6.3.2, effective 2012).

**Media Protection:** Media protection policy and procedures must be documented and implemented to ensure access to media in all forms is restricted to authorized individuals. Procedures must be defined for securely handling, transporting, and storing media (CJIS Security Policy Section 5.8).

**Sanitization/Disposal of Electronic Media:** The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media (CJIS Security Policy Section 5.8.3).

**Disposal of Physical Media:** Formal procedures must be in place for the secure disposal or destruction of physical media by shredding or incineration (CJIS Security Policy Section 5.8.4).

**Physical Protection:** Physical protection policy and procedures must be documented to ensure criminal justice information system hardware, software, and media are physically protected (CJIS Security Policy Section 5.9).

**Patch Management:** The agency must develop and implement a local policy that ensures prompt installation of newly released security relevant patches, service packs and hot fixes (CJIS Security Policy Section 5.10.4.1).

**Personnel Sanctions:** Agencies must employ a formal sanctions process for personnel failing to comply with established system policies and procedures (CJIS Security Policy Section 5.12.4).

## Timetable

Each coming year has important deadlines for implementation of specific requirements of the CJIS Security Policy. A timeline of these is provided to help you look ahead and plan for these important changes.

|      |  |
|------|--|
| 2012 | Specific requirements for managing information security incident response (Section 5.3)  |
|      | Additional language regarding information security is required in agency agreements (Section 5.3)  |
|      | Numerous requirements for wireless protocols (Section 5.5)   |
|      | Must validate user accounts annually and document the process (Section 5.5)  |
|      | Access to privileged functions must be restricted to explicitly authorized personnel (Section 5.5)   |
|      | Identifier and authenticator management process must be documented (Section 5.6)   |
|      | Visitor access logs must be maintained at least one year and must include the name and agency of the visitor, their signature, what form of identification was used to identify the visitor, date of access, time of entry and departure, purpose of their visit and name and agency of who they visited (Section 5.9) |
|      | Specific requirements for partitioning (Section 5.10)  |
|      | Specific requirements for virtualization (Section 5.10)  |
|      | Security alert/advisory procedures must be in place (Section 5.10)   |
| 2013 | Security awareness training required for all who access or receive criminal justice information (Section 5.2)  |
|      | Automated process required when possible to support security incident response (Section 5.3)   |
|      | Specific information must be logged regarding specific computer events, these audit records must be time stamped when generated (Section 5.4)  |
|      | System must be in place to alert agency if logging fails (Section 5.4)   |
|      | Event logs must be reviewed at least once a week, and these audit records must be retained until no longer needed (Section 5.4)  |
|      | Additional access control policies must be in place (Section 5.5)  |
|      | Users must acknowledge a system use notification before login (Section 5.5)  |
|      | Use of existing VPNs with IPSec to meet Advanced Authentication requirements from a police vehicle no longer allowed (Section 5.6)   |
|      | Encryption of stored data required if agency cannot meet physical and personnel security requirements (Section 5.8)  |
|      | Monitoring/boundary protection required (Section 5.10)   |
|      | Information must be encrypted if at rest outside the boundary of the physically secure location (Section 5.10)   |
|      | Network based intrusion detection tools and techniques must be employed (Section 5.10)   |
| 2014 | Requirements for use of assertions (Section 5.6)   |