June 26, 2017

SECURITY & ACCESS SECTION
2016 Information Technology Security Audit
Criminal Justice Agencies

This correspondence has been created to communicate the results of Michigan's 2016 Information Technology Security Audit (ITSA) conducted by the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Audit Unit.

The FBI conducts a triennial ITSA of each CJIS Systems Agency (CSA) to verify compliance with the FBI CJIS Security Policy. The audit reviews compliance through the assessment of a number of local criminal justice agencies (CJA) as well as noncriminal justice agencies (NCJA) receiving FBI-provided criminal justice information (CJI) services through the CSA. The CSA for Michigan is the Michigan State Police. For 2016, the FBI assessed 12 CJAs and five NCJAs to ensure policy compliance at the CSA level.

Below is a list of noncompliant areas found in the Michigan audit and the specific finding in each area.

Private Contractor User Agreements and CJIS Security Addendum
CJIS Security Policy: "All private contractors who perform criminal justice functions shall acknowledge, via signing of the CJIS Security Addendum Certification page, and abide by all aspects of the CJIS Security Addendum."

Finding(s):

- The Security Addendum was not signed by contactor personnel that performed unescorted shredding services.

Analysis: This is not an unusual finding in relation to shredding service providers. Options to remedy this finding include required addendums being signed; bringing contracted shredding services on-site where they can be witnessed by an authorized staff member; or conducting shredding in-house by authorized personnel.

Security Awareness Training

CJIS Security Policy: “Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI.”

Finding(s):

- Security Awareness Training was not provided to:
  - Criminal justice agency personnel
  - City information technology (IT) personnel
  - Contractors that performed unescorted shredding services
  - Vendor personnel with unescorted access to the physically secure location
  - Noncriminal justice agency personnel with unescorted access to the physically secure location

Analysis: This is not an unusual finding in relation to personnel who have access to physically secure locations but no perceived access to CJI. Examples include janitorial and maintenance personnel, as well as IT personnel who service the information systems that process and store CJI. Agencies should have all personnel with access to the physically secure location take security awareness training, document that training, and maintain the biennial training requirement. Shredding company personnel can either take the training or the agency can elect to have authorized personnel witness or perform the shredding.

Auditing and Accountability

CJIS Security Policy: “Agencies shall implement audit and accountability controls to increase the probability of authorized users conforming to a prescribed pattern of behavior. Agencies shall carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components.”

Finding(s):

  - All appropriate events were not logged for information systems processing, storing, and transmitting CJI
  - Information system audit logs were not retained for the minimum of one year

Analysis: This area has only more recently become a focus area of the FBI when conducting assessments. While most agencies are collecting some form of audit information, it was discovered that some were not necessarily collecting all the required information. See CJIS Security Policy section 5.4.1 for a specific list of system events and content required to be audited. Additionally, a number of the agencies were maintaining audit records, but for less than the required 365 minimum retention period.

Passwords

CJIS Security Policy: “Agencies shall follow the secure password attributes…to authenticate an individual’s unique ID.

Finding(s):

- Passwords used to access, process, store or transmit CJI were non-compliant on:
  - Windows Active Directory
  - Live Scan devices
  - Mugshot applications
  - Mobile Data Computer application

Analysis: The primary areas of concern were systems that did not meet the secure attribute requirements of policy; either Live Scan and mugshot systems, or Windows Active Directory. Agencies should refer to CJIS Security Policy section 5.6.2.1.1 for a complete listing of FBI requirements for secure password attributes.

Media Protection
CJIS Security Policy: "Media protection policy and procedures shall be documented and implemented to ensure that access to digital and physical media in all forms is restricted to authorized individuals. Procedures shall be defined for securely handling, transporting and storing media."

Finding(s):

- Agencies did not have a written policy for:
  - Sanitization and destruction process of physical and electronic media

- Agency did not witness:
  - Disposal and destruction of physical and electronic media carried out by unauthorized personnel

Analysis: A few agencies failed to have a documented policy for the sanitization and destruction of media. These agencies were compliant in the actual function, but not compliant in that they did not have a policy and process. Additionally, one agency was sending their physical media offsite for destruction and were not witnessing the destruction process.

Boundary Protection
CJIS Security Policy: "The agency shall:
Control access to networks processing CJI.

1. *Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.*
2. *Ensure any connections to the Internet, other external networks, or information systems occur through controlled interfaces (e.g. proxies, gateways, routers, firewalls, encrypted tunnels). See Section 5.13.4.4 for guidance on personal firewalls.*
3. *Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use.*
4. *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").*
5. *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."*

Finding(s):

- The boundary protection was not patched with an available update
- The firewall configuration was not backed up

Analysis: In the area of boundary protection, one of the agencies was unable to provide the evidence that they had employed the most recent patches and updates to their systems. Another did not have adequate protections in place to separate the CJA and NCJA portions of their network infrastructure. Finally, one agency was not backing up their firewall configuration on a frequent basis.

Encryption

CJIS Security Policy: "Commonly available encryption tools often use a key to unlock the cipher to allow data access; this key is called a passphrase. While similar to a password, a passphrase is not used for user authentication. Additionally, the passphrase contains stringent character requirements making it more secure and thus providing a higher level of confidence that the passphrase will not be compromised.

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).*
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."*

Finding(s):

- Encryption for transmitting CJI outside the physically secure location was noncompliant on:
    - A city network
    - A county network
    - From the police department to substations
    - From the criminal justice agency to a backup location
    - Remote access software used to access CJI

Analysis: Encryption is frequently an area of noncompliance with agencies. The reasons range from a misunderstanding of the policy requirements for network segments to an agency being unable to produce evidence that the encryption used meets the NIST requirement. Six agencies had some form of noncompliance with the policy encryption requirement. Of those, four were utilizing encryption but were unable to provide the required FIPS 140-2 certificate; two were found noncompliant for failing to have encryption in transit on segments of their city and county networks.

Patch Management*

CJIS Security Policy: "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."

Finding(s):

- Windows XP no longer supported by Microsoft
- Windows Server 2003 no longer supported by Microsoft

Analysis: Five agencies were found to still be utilizing either Windows XP machines or Windows Server 2003 which are both end-of-life and no longer supported.

*While not evaluated at audit, effective April 11, 2017, Windows Vista is no longer supported by Microsoft.

Personnel Security

CJIS Security Policy: "Having proper security measures against the insider threat is a critical component for the CJIS Security Policy. This section's security terms and requirements apply to all personnel who have access to unencrypted CJI including those individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI."

Finding(s):

- Agencies did not fingerprint:
  - City IT personnel
  - Janitorial Personnel
  - Contractors that performed unescorted shredding services
  - Noncriminal justice personnel with unescorted access to the physically secure location

Analysis: Much like security awareness training, agencies sometimes overlook fingerprinting personnel or contractors/vendors whom they perceive as having no access to CJI. During the 2016 FBI ITSA, three agencies were found noncompliant. One agency failed to fingerprint and background check an offsite paper shredding company; one neglected to fingerprint and background check their city IT staff; and the last agency missed its janitorial and telecomm staff. As with security awareness training and security addendums, this finding for unauthorized personnel performing shredding services can be remediated by authorized personnel witnessing the shredding or authorized agency personnel performing the shredding.