2019 Federal Bureau of Investigation Information Technology Security Audit of Michigan
Summary of Findings

Criminal Justice Agencies

This correspondence provides the results of the 2019 Federal Bureau of Investigation (FBI) Information Technology (IT) Security Audit of Michigan. The Michigan State Police (MSP), as the Criminal Justice Information Services (CJIS) Systems Agency (CSA) for the state of Michigan, is audited every three years. As part of the audit, 14 local criminal justice agencies were selected to participate in a local agency review.

Below is a summary of the findings in Michigan:

Ensure the local agencies implement all audit and accountability controls for information systems accessing CJI. *(This was a finding at four local agencies and has been a finding in the two previous FBI audit cycles.)*
(*CJIS Security Policy*, Version 5.7, August 2018, 5 Policy and Implementation, 5.4 Policy Area 4: Auditing and Accountability, 5.4.1 Auditable Events and Content (Information Systems), pp. 27-28.)

Findings:

- Programs with access to CJI not logging all required events.
- Program with access to CJI not logging any required events.
    - *Remediation: Agencies have either implemented, or are currently implementing, software changes to ensure that all required events and associated content are being captured.*
- Local agencies not reviewing system audit logs at a minimum of once a week for inappropriate, unusual, or suspicious activity.
    - *Remediation: Agencies have added weekly log review to their information technology standard operating procedures.*

Ensure CJI transmitted or stored outside the boundary of the physically secure location is immediately protected via encryption to comply with the *CJIS Security Policy* requirements. *(This was a finding at five local agencies and has been a finding in the two previous FBI audit cycles.)*
(*CJIS Security Policy*, Version 5.7, August 2015, 5 Policy and Implementation, 5.10 Policy Area 10: System and Communications Protection and Information Integrity, 5.10.1.2 Encryption, 5.10.1.2.1 Encryption for CJI in Transit pp. 54-55.)

Findings:

- Unable to provide verification that e-mails transmitted over the Internet were encrypted with at least 128-bit National Institute for Standards and Technology (NIST) certified encryption.
    - *Remediation: Agency has stopped utilizing email for transfer of documents containing CJI.*
- Unable to provide verification that either the data or the network segment transmitting information system backups containing CJI were encrypted between physically secure locations.
- Unable to provide verification that either the data or network segment transmitting CJI from local agency to agency data center were encrypted in transit.
    - *Remediation: Agency purchased and is in the process of implementing equipment that provides building-to-building encryption meeting FIPS certification requirement.*
- Unable to provide verification that encryption utilized by IT administrators for remote access and maintenance was at least 128-bit Federal Information Processing Standards (FIPS) certified.
    - *Remediation: After completion of audit, agency IT staff were able to provide documentation of appropriate remote access mechanisms.*

Ensure local agencies implement security controls on their virtual environment that hosts CJI.
(This was a finding at three local agencies.)
(*CJIS Security Policy*, Version 5.7, August 2018, 5 Policy and Implementation, 5.10 Policy Area 10: System and Communications Protection and Information Integrity, 5.10.3 Partitioning and Virtualization, pp. 57-58.)

Findings:

- Local agency did not partition CJI-related information systems or applications on a shared host containing non-CJI related systems or applications.
    - *Remediation: The agency purchased a server dedicated to hosting CJI-related information systems or applications separately from noncriminal justice information systems or applications.*
- Audit logs for CJI applications hosted in a virtual environment were not stored outside of the hosts virtual environment.
    - *Remediation: Agency provided proof of compliance after the audit.*

The FBI's CJIS Division is authorized to conduct an IT Security Audit of the CSA, at least once every three (3) years at a minimum, to assess agency compliance with the CJIS Security Policy on all networks and information systems which access, transmit, or store criminal justice information (CJI). The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information. Policies and procedures governing the security of CJI are examined during the audits. Assessments are made based on policies set forth in the CJIS Security Policy; Advisory Policy Board Bylaws and meeting minutes; and applicable federal laws. Although compliance with every requirement of the CJIS Security Policy was not assessed, adherence to all security policies and procedures contained with the CJIS Security Policy is required for FBI CJIS systems access.

During the audit, the FBI utilized the CJIS Security Policy, Version 5.7, published August 16, 2018. The references above reflect this version. Revisions are published on an annual basis and agencies are responsible for complying with the requirements in the most current version. The current CJIS Security Policy version is available at: https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center.