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

Noncriminal 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, seven local noncriminal justice agencies were selected to participate in a local agency review.

Below is a summary of the findings in Michigan:

Ensure local agencies request and receive written permission from the State Compact Officer or Chief Administrator prior to executing a contract or agreement that permits a contractor to access national Criminal History Record Information (CHRI).
(*CJIS Security Policy*, Version 5.7, August 2018, 5 Policy and Implementation, 5.1 Policy Area 1: Information Exchange Agreements, 5.1.1 Information Exchange, 5.1.1.8 Outsourcing Standards for Non-Channelers, p. 18.)

Findings:

- Local agency did not request or receive permission from the state Compact Officer prior to outsourcing noncriminal justice functions that allowed contractor personnel unescorted access to CHRI.
    - *Remediation: Agency and the MSP are currently working together to remediate the finding.*

Ensure that CJI transmitted outside the boundary of the physically secure location is immediately protected via encryption to comply with *CJIS Security Policy* requirements. *(This is a finding at two 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, 5.10.1.2 Encryption, 5.10.1.2.1 Encryption for CJI in Transit, pp. 54-55.)

Findings:

- Local agency was unable to provide verification that either the data or the network segment transmitting information backups containing CHRI was encrypted in transit between physically secure locations.
    - *Remediation: Agency moved all digitally stored CHRI off network to paper files and has begun to utilize the Criminal History Record Internet Subscription Service (CHRISS) for access and review of future CHRI.*
- Local agency was unable to provide a Federal Information Processing Standards (FIPS) 140-2 certificate associated with agency's authorized users at one agency location access to CHRI indicators stored within a server located in another facility.
    - *Remediation: The local agency provided the FIPS certificate at a later date.*

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.