



John Watson
Missouri State Auditor

HIGHWAY PATROL

Criminal Justice Information Security Management



April 2015
Report No. 2015-019

<http://auditor.mo.gov>



John Watson
Missouri State Auditor

CITIZENS SUMMARY

Findings in the audit of the Department of Public Safety, Missouri State Highway Patrol, Criminal Justice Information Security Management

Recusal	To avoid any appearance of a conflict of interest, the State Auditor recused himself from participation in this audit and directed the Deputy State Auditor to oversee procedures performed by the State Auditor's professional audit staff.
Background	The Missouri Department of Public Safety - Missouri State Highway Patrol (MSHP) is responsible for administering the systems and infrastructure for maintaining and disseminating criminal justice information (CJI) used by agencies for criminal justice and certain noncriminal justice purposes. The MSHP has been designated as Missouri's Criminal Justice Information Services (CJIS) Systems Agency by the United States Department of Justice Federal Bureau of Investigation (FBI) and is responsible for establishing and administering an information technology security program for users, including local agencies. The Missouri Uniform Law Enforcement System (MULES) is a statewide computerized communications system managed by the MSHP designed to provide services, information, and capabilities to the law enforcement and criminal justice community in Missouri. The MULES is used by the state to meet FBI requirements and serves as the central system for providing criminal justice agencies and certain noncriminal justice agencies with access to federal, state, and local CJI through the CJIS network.
Agency Compliance Controls	MSHP management has taken significant steps to protect information systems from threats. However, opportunities exist to strengthen the MSHP's security posture. The MSHP has not fully established policies and procedures to proactively monitor the activity or events performed by MULES users, and does not have adequate procedures for reporting, tracking, and monitoring incidents of inappropriate use. The MSHP has not performed security audits since July 2012, and does not have adequate policies or procedures for performing policy compliance review (PCR) audits to ensure agency compliance with the National Crime Information Center and MULES policies. The MSHP also does not centrally track the results of PCR audits performed. In addition, the MSHP does not require regular background checks of MSHP users with access to the MULES. The MSHP has not entered into user agreements with some agencies that have access to CJI, and has not ensured that all agreements meet federal and state requirements. Further, the MSHP has not ensured all users with access to CJI are sufficiently trained and aware of their security responsibilities.
User Account Management	The MSHP has not fully established policies and procedures for requesting, granting, and removing access to the CJIS network, the MULES, or other supporting systems. The MSHP has not fully established procedures for administering and reviewing user access to data and other information resources to ensure access rights relate with job duties. Reviews are not regularly performed to identify terminated or transferred users with access to the CJIS network or the MULES, or to determine whether disabled accounts can be permanently removed. As of November 2014, twenty former MSHP employees still had access to the MULES, and MSHP officials maintained 13,200 disabled MULES user accounts. MSHP officials also did not provide supervisory oversight or establish other mitigating controls to ensure users with extensive access rights did not perform unauthorized tasks. In addition, users that

remotely access the MULES (56 percent of users) are not required to follow certain security controls required of users accessing the MULES directly. Also, MSHP management has not fully documented access profiles that may be assigned to MULES users.

Information Security Program	MSHP management has made several significant improvements to the information security program since 2012. However, the MSHP has not established a comprehensive risk assessment and management program to identify potential threats and vulnerabilities. In addition, an incident response plan has not been fully established to ensure computer security incidents are correctly logged, analyzed, and appropriate action is taken. The MSHP has not defined the security events to be logged and reviewed and the MULES does not have the capability to track user additions, changes, or deletions. MSHP management has not consistently ensured all users are uniquely identified or that passwords are not shared and are changed every 90 days. The MULES does not have controls to limit the number of consecutive unsuccessful access attempts and management has not established formal written policies to periodically review and evaluate the effectiveness of security settings for the MULES or the CJIS network. The MSHP does not have sufficient physical security policies and procedures to ensure computer resources are properly controlled, monitored, and restricted to authorized individuals. Further, the MSHP has not fully established or documented policies and procedures for the sanitization and destruction of electronic media containing CJI, has not fully documented the roles and responsibilities for several employees responsible for information security, and has not fully established procedures for reviewing and re-approving key standards, directives, policies, or procedures related to information technology and security.
Disaster Recovery Plan	The MSHP's Disaster Recovery Plan does not include certain needed information should a disaster occur. Although the MSHP has implemented and tested some recovery procedures, the plan is not complete and has not been updated to reflect changes in the operating environment. In addition, a comprehensive test to ensure critical systems can be fully restored has not been performed.
National Data Exchange	The MSHP has not performed audits of agencies with direct access to the National Data Exchange System (N-DEx) to ensure compliance with applicable statutes, regulations, and policies. In addition, management has not established procedures to ensure that N-DEx users receive biennial security awareness training.

In the areas audited, the overall performance of this entity was **Fair**.*

*The rating(s) cover only audited areas and do not reflect an opinion on the overall operation of the entity. Within that context, the rating scale indicates the following:

- Excellent:** The audit results indicate this entity is very well managed. The report contains no findings. In addition, if applicable, prior recommendations have been implemented.
- Good:** The audit results indicate this entity is well managed. The report contains few findings, and the entity has indicated most or all recommendations have already been, or will be, implemented. In addition, if applicable, many of the prior recommendations have been implemented.
- Fair:** The audit results indicate this entity needs to improve operations in several areas. The report contains several findings, or one or more findings that require management's immediate attention, and/or the entity has indicated several recommendations will not be implemented. In addition, if applicable, several prior recommendations have not been implemented.
- Poor:** The audit results indicate this entity needs to significantly improve operations. The report contains numerous findings that require management's immediate attention, and/or the entity has indicated most recommendations will not be implemented. In addition, if applicable, most prior recommendations have not been implemented.

All reports are available on our Web site: auditor.mo.gov

Criminal Justice Information Security Management

Table of Contents

State Auditor's Report	2
------------------------	---

Introduction	
Background	4
Missouri Uniform Law Enforcement System (MULES)	5
Scope and Methodology.....	7

Management Advisory Report - State Auditor's Findings	
1. Agency Compliance Controls	9
2. User Account Management	21
3. Information Security Program.....	29
4. Disaster Recovery Plan	38
5. National Data Exchange	39



JOHN WATSON

Missouri State Auditor

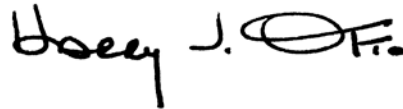
Honorable Jeremiah W. (Jay) Nixon, Governor
and
Peter Lyskowski, Acting Director
Department of Public Safety
and
Colonel Ronald K. Replogle, Superintendent
Missouri State Highway Patrol
Jefferson City, Missouri

To avoid any appearance of a conflict of interest, the State Auditor recused himself from participation in this audit and directed the Deputy State Auditor to oversee procedures performed by the State Auditor's professional audit staff. We have audited the Department of Public Safety-Missouri State Highway Patrol management of security controls related to criminal justice information in fulfillment of our duties under Chapter 29, RSMo. This audit was conducted to evaluate the effectiveness of security controls and other related internal controls designed to secure confidential criminal justice information and as a result of increasing concerns regarding security of information maintained in state databases. The objectives of our audit were to:

1. Evaluate internal controls over significant management and financial functions.
2. Evaluate compliance with certain legal provisions.
3. Evaluate the economy and efficiency of certain management practices and information system control activities.
4. Evaluate the effectiveness of information security controls for protecting the confidentiality, integrity, and availability of significant systems and information.

We conducted our audit in accordance with the standards applicable to performance audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States. Those standards require that we plan and perform our audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides such a basis.

For the areas audited, we identified (1) deficiencies in internal controls, (2) no significant noncompliance with legal provisions, (3) the need for improvement in management policies and procedures, and (4) the need to fully implement an information security program and related security controls. The accompanying Management Advisory Report presents our findings arising from our audit of the Department of Public Safety - Missouri State Highway Patrol.

A handwritten signature in black ink, appearing to read "Harry J. Otto". The signature is stylized with a large, looped "H" and a cursive "O".

Harry J. Otto, CPA
Deputy State Auditor

The following auditors participated in the preparation of this report:

Director of Audits:	John Luetkemeyer, CPA
Audit Manager:	Jeffrey Thelen, CPA, CISA
In-Charge Auditor:	Amanda Locke, M.Acct. Patrick M. Pullins, M.Acct., CISA
Audit Staff:	Jill Wilson, MBA

Criminal Justice Information Security Management

Introduction

Background

The Missouri Department of Public Safety - Missouri State Highway Patrol (MSHP) is responsible for administering the systems and infrastructure for maintaining and disseminating criminal justice information (CJI) used by agencies for criminal justice and certain noncriminal justice purposes. The MSHP relies extensively on information systems to support mission-related operations and on information security controls to protect the confidentiality, integrity, and availability of sensitive CJI maintained in those systems.

Information security is a critical consideration for any organization dependent on information systems and networks to meet its mission or business objectives. Information security is especially important for state agencies, where public trust is essential for the efficient delivery of services. Security can be a significant investment, which adds to an already long list of administrative duties. Managing secure networks, developing and implementing new system functionality, maintaining system users, and other day-to-day security tasks can strain limited administrative resources. However, agency management must understand proper protection of citizen information is a requirement and not a luxury in the current interconnected cyber environment. Without proper safeguards and controls, computer systems and confidential data are vulnerable to individuals with malicious intentions who can use access to obtain sensitive data or disrupt operations.

The MSHP mission is to serve and protect all people by enforcing laws and providing services to ensure a safe and secure environment. The MSHP has been designated as Missouri's Criminal Justice Information Services (CJIS) Systems Agency (CSA) by the United States Department of Justice Federal Bureau of Investigation (FBI) and is responsible for establishing and administering an information technology security program for users, including local agencies. The MSHP is organized into five bureaus, which are comprised of several divisions and troops. The CJIS Division and the Information and Communications Technology Division (ICTD) are within the Technical Services Bureau.

The CJIS Division has been designated as the Central Repository for Missouri, which according to Section 43.500, RSMo, is responsible for compiling and disseminating complete and accurate criminal history records. In addition, the CJIS Division is responsible for ensuring agencies that utilize CJI are in compliance with federal and state laws, regulations, and policies. The ICTD is responsible for developing and maintaining computer systems for criminal justice agencies at both the state and local levels of government.

CJIS Division and ICTD management have primary responsibility for administration and oversight of the policies and procedures for security and control of department information systems and technology resources. MSHP



Criminal Justice Information Security Management Introduction

staff and personnel at other agencies are responsible for performing duties required by applicable requirements.

Missouri Uniform Law Enforcement System

The Missouri Uniform Law Enforcement System (MULES) is managed by the MSHP. Section 43.010, RSMo, states MULES is a statewide-computerized communications system designed to provide services, information, and capabilities to the law enforcement and criminal justice community in Missouri. The MULES is the state's single point of entry into the National Crime Information Center (NCIC), the criminal justice information system operated by the FBI. The MULES is used by the state to meet FBI requirements and serves as the central system for providing criminal justice agencies and certain noncriminal justice agencies with access to federal, state, and local CJI through the CJIS network.

According to the CJIS Security Policy,¹ CJI is the term used to refer to all of the federal CJIS data necessary for law enforcement and civil agencies to perform their missions including, but not limited to, biometric, identity history, biographic, property, and case/incident history data. Some of the CJI collected, maintained and accessible to users of the MULES includes:

- Missouri hot file data, such as wanted persons, missing persons, orders of protection, stolen license plates, towed vehicles, and stolen property.
- Federal data from the NCIC, including hot file data, gang file data, suspected terrorists, violent persons, and national sexual offender registry files.
- Missouri criminal history record information (CHRI), such as arrests, prosecutor and court actions, dispositions, and incarceration records.
- Federal and other state CHRI, or data available from the Interstate Identification Index, such as names and personal identification information of arrested persons.
- Missouri sexual offender registry information, such as listings of persons found guilty of sexual and certain other offenses.
- Missouri Department of Revenue (DOR) driver's license data, such as demographic information, photographs, and driving records of cardholders.
- Missouri DOR motor vehicle data, such as license plate numbers, owners, and registration statuses of vehicles.
- Data from the National Law Enforcement Telecommunications System (NLETS), such as hot file data, CHRI, warrant, driver license data, and motor vehicle data from other state, federal, and Canadian agencies.

¹ U.S. Department of Justice Federal Bureau of Investigation Criminal Justice Information Services Division, Criminal Justice Information Services (CJIS) Security Policy Version 5.2.



Criminal Justice Information Security Management Introduction

- Missouri Department of Corrections (DOC) data, such as information on prisoners confined at a Missouri DOC facility or individuals under the supervision of a Missouri Probation and Parole office.

Some of the major functionality available in the MULES includes the ability for users to enter, maintain, and inquire on records of interest. In addition, the system allows users to search various sources of information simultaneously. For example, users could enter a single set of search criteria, such as a last name and date of birth, and search multiple Missouri and federal data sources simultaneously, such as the hot files, CHRI, driver's licenses, motor vehicles, and sexual offender registries.

CJI is used for both criminal justice and noncriminal justice purposes. Federal and/or state laws and regulations indicate agencies such as Police Departments, Sheriff's offices, Departments of Corrections, Prosecuting Attorney's offices, municipal or state courts, and contractors with a criminal justice purpose may have access to CJI. In Missouri, the MSHP allows authorized personnel at these agencies to have direct access to the MULES. In addition, noncriminal justice agencies such as certain state agencies, school districts, and nursing homes are authorized by federal or state law to receive civil fingerprint-based background checks for employment, licensing determinations, immigration and naturalization matters, and national security clearances. For example, since state law requires school districts to ensure applicants for most school district positions have a criminal history background check performed prior to having contact with a student, certain personnel at the school districts are authorized access to CJI. In Missouri, these agencies do not have direct access to the MULES, but upon requesting the fingerprint-based background check from the MSHP, are provided access to the results of the request using data generated from the MULES.

Security and access controls

According to accepted standards, security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. Confidentiality refers to preserving authorized restrictions on information access and disclosure, including the means for protecting personal privacy and proprietary information. Integrity relates to guarding against improper information modification or destruction, and availability ensures timely and reliable access to and use of information.

MSHP management is responsible for ensuring the confidentiality and privacy of the CJI collected, maintained, used, or transmitted from the MULES and other connected systems by establishing effective security and access controls. Security of CJI is especially important when such information can be directly linked to an individual. Confidentiality is



Criminal Justice Information Security Management Introduction

threatened not only by the risk of improper access to electronically stored information, but also by the risk of interception during electronic transmission of the information.

The MULES is a private network information system that can be accessed by authorized users. Access to MULES is controlled using various resources, including the networks, security system, and/or remote access mechanisms. The MULES security system controls the level of access a user is granted, including the actions a user can perform. The CJIS Division and the ICTD also use internal databases or systems to store user account information and to track user access to the MULES and other resources, agency information, and training records for MULES users.

Requirements

The CJI accessible through the MULES and other systems contains personally identifiable information (PII), such as social security numbers (SSN), and other legal information. Federal² and state³ policies require criminal justice agencies to ensure appropriate safeguards are in place to protect the confidentiality, integrity, and availability of CJI.

Federal and state law, regulations, and policies govern the access, use, and dissemination of CJI. Improper access, use or dissemination of information is serious and may result in sanctions including, but not limited to, termination of services, and state and/or federal criminal and civil penalties. Inappropriate use of CJI could include an individual accessing the MULES under access privileges associated with an agency for which he or she no longer works; an individual using the information for personal use or private gain, in exchange for monetary or other compensation; and disseminating information to an individual outside of the criminal justice system.

Scope and Methodology

The scope of our audit included information security and other relevant internal controls, policies and procedures, and other management functions and compliance issues in place during the year ended June 30, 2014.

Our methodology included conducting interviews with appropriate officials and staff, as well as certain external parties; identifying, obtaining, and reviewing available written policies and procedures, federal and state laws, and other applicable information; and performing testing.

² U.S. Department of Justice Federal Bureau of Investigation National Crime Information Center (NCIC) Division, NCIC 2000 Operating Manual. The NCIC is a nationwide, computerized information system containing CJI available to all criminal justice agencies. NCIC policy establishes a number of security measures to ensure the privacy and integrity of the data. In addition, NCIC policy requires data to be complete, accurate, and entered timely.

³ The Missouri Uniform Law Enforcement System Policy and Standards Manual (MULES Policy) is the MSHP supplement to the CJIS Security Policy and the NCIC Policy.



Criminal Justice Information Security Management Introduction

We obtained a data file from MSHP officials of user accounts having access to the MULES as of November 2014. To ensure completeness of the data, we grouped the accounts by agency and reviewed for reasonableness. Although we used computer-processed data from the MULES for our audit work, we did not rely on the results of any processes performed by this system in arriving at our conclusions. Our conclusions were based on our review and testing of the issues specific to the audit objectives.

We obtained employment records of all MSHP employees from the statewide accounting system for human resources. We matched these records to MULES user accounts to determine if any terminated employees had active user accounts. We gave MSHP officials a list of all terminated employees we found who had active access to the MULES. Although we used computer-processed data from the statewide accounting system for our audit work, we did not rely on the results of any processes performed by this system in arriving at our conclusions. Our conclusions were based on our review and testing of the issues specific to the audit objectives.

To assess the reliability of other data and information we analyzed, such as system control settings, compliance audits, authorization documents, and security policies and procedures, we corroborated the information with MSHP officials and security administrators to determine whether the data obtained were consistent with system configurations and controls in place at the time of our review. Based on this assessment, we determined the data and information were reliable for the purposes of this report.

We based our evaluation on accepted state, federal, and international standards, policies and procedures, and best practices related to information technology security controls from the following sources:

- CJIS Security Policy Version 5.2
- NCIC 2000 Operating Manual
- MULES policy
- National Institute of Standards and Technology (NIST)
- Government Accountability Office (GAO)
- ISACA (previously known as the Information Systems Audit and Control Association)

Criminal Justice Information Security Management

Management Advisory Report

State Auditor's Findings

1. Agency Compliance Controls

While Missouri State Highway Patrol (MSHP) management has taken significant steps to protect information systems from threats, opportunities exist to strengthen the agency's security posture and reduce security risk by enhancing agency compliance controls.

According to MSHP officials, the following steps have been taken to improve the overall security of the MSHP's information systems:

- The creation of an Information Security Unit dedicated solely to information security operations and ensuring compliance by federal, state, and local user agencies.
- The appointment of a Chief Information Security Officer, responsible to direct oversight of cybersecurity operations and overall day-to-day information security governance.
- The development of a comprehensive information security strategy linking security policies and protections to agency operational needs.
- A significant investment in a security architecture designed to provide protection to critical data and other assets from known and emerging threats.
- Training and auditing programs aimed at ensuring compliance with various statutory and regulatory requirements.
- Outreach programs providing expertise and security related training to law enforcement agencies of all sizes.

MSHP management needs to improve controls and procedures to ensure agencies are in compliance with information security standards, applicable laws, regulations, and requirements for protecting the generation, transmission, and storage of criminal justice information (CJI). MSHP management has generally developed many of the controls needed to assess agency compliance with requirements, but these control requirements have not been fully implemented.

The Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy states the CJIS Systems Agency⁴ (CSA) is responsible for establishing and administering an information technology security program throughout the CSA's user community, to include the local

⁴ The FBI has designated the Missouri State Highway Patrol as the CJIS Systems Agency (CSA) for Missouri.



Criminal Justice Information Security Management Management Advisory Report - State Auditor's Finding

levels.⁵ Each agency is responsible for ensuring the protection of CJI and complying with federal and state requirements. For example, the CJIS Security Policy states controls shall be established to protect information from unauthorized disclosure, alteration or misuse. The CSA is ultimately responsible for ensuring each agency is in compliance with federal and state requirements.

As the CSA, the MSHP has a demanding responsibility for administering and monitoring the information security program and compliance components to ensure federal and state requirements are complied with by both MSHP and local agency personnel. A MSHP official indicated 792 agencies had direct access to the MULES as of October 2014, and our review identified 21,169 active MULES user accounts as of November 2014. The MSHP is also responsible for monitoring approximately 800 noncriminal justice agencies authorized to access CJI. As a result, significant resources are necessary for the MSHP to meet CSA objectives and compliance requirements.

However, without adequate monitoring and control procedures, management faces an increased risk that appropriate controls for protecting the full lifecycle of CJI have not been effectively implemented, which jeopardizes the reliability, confidentiality, completeness, and accuracy of information maintained by the CJIS system, including the MULES.

1.1 Monitoring and handling incidents of inappropriate use of CJI

MSHP management needs to improve controls and procedures to fully ensure (1) CJI is used in accordance with federal and state requirements and (2) incidents of potential inappropriate use of CJI are tracked and handled. The CJIS Security Policy requires the CJIS Systems Officer (CSO) at the CSA to ensure appropriate use, enforce system discipline, and ensure CJIS Division operating procedures are followed by all users of the respective services and information.

Audit trail monitoring

MSHP management has not fully established policies and procedures to proactively monitor the activity or events performed by Missouri Uniform Law Enforcement System (MULES) users. The MULES logs all criminal history inquiries by maintaining a record of every transaction made. However, a MSHP official said due to the large number of transactions generated by MULES users and insufficient resources, the MSHP has not been able to do much proactive monitoring for unusual or inappropriate activity on a regular basis. Instead, the MSHP relies upon a shared compliance enforcement approach with local agencies and reviews of audit

⁵ The local levels (agencies) in Missouri refer to local criminal justice agencies (such as Police Departments, Sheriff's offices, courts, etc.) or noncriminal justice agencies designated to perform criminal justice functions (such as a city information technology department).



Criminal Justice Information Security Management Management Advisory Report - State Auditor's Finding

trail records performed during triennial policy compliance reviews (PCR) to determine if inappropriate activity occurred. According to a MSHP official, other monitoring reviews are performed but are more reactive, or based upon inquiries from employers and other individuals about potential instances of inappropriate use of CJI. In addition, the MSHP now requires agencies to report inappropriate use of CJI within 24 hours of becoming aware of the misuse.

Audit and monitoring involves the regular collection, review, and analysis of auditable events for indications of inappropriate or unusual activity, and the appropriate investigation and reporting of such activity, according to the Government Accountability Office (GAO). Monitoring of activity and usage of CJI is necessary to identify improper access, use, or dissemination of CJI, including noncompliance with federal and state requirements. The loss or unauthorized disclosure or alteration of the information residing on systems, which can include personally identifiable information (PII), can lead to serious consequences and substantial harm to individuals and the nation, according to the GAO. Further, the lack of frequent reviews of audit trail information may result in significant instances of misuse not being detected.

Incident response

MSHP management has not fully established or standardized procedures for reporting, tracking, and monitoring incidents of inappropriate use⁶ of CJI. MSHP personnel learn of potential inappropriate use of CJI through various sources, such as notifications from federal agency personnel, CJIS audit staff, local agency personnel, or private citizens. For example, a local agency may request audit trail records from the MSHP to determine if a user improperly accessed CJI.

A MSHP official said a centralized method to document reports of potential misuse, or to track the status and results of those incidents had not been established. The MSHP documented the number of audit trail record requests received from local agencies for investigating potential misuse of CJI. However, the status of those requests, including whether actual misuse was identified, was not tracked. As a result, MSHP management was unable to statistically assess the extent and nature of misuse of CJI. A MSHP official said recent improvements have been made to enhance the overall response to incidents of inappropriate use. In the fall of 2013 the MSHP issued a new state policy requiring that agencies report any security incident, including inappropriate use within 24 hours of discovery. In addition, in the fall of 2014, a security incident reporting system was implemented allowing agencies to electronically report security incidents.

⁶ Inappropriate use includes accessing CJI for private or personal use, for a purpose other than in connection with official duties and job-related performance, or with invalid access privileges.



Criminal Justice Information Security Management Management Advisory Report - State Auditor's Finding

Submissions to this system result in immediate notification to MSHP staff and creates a database entry for incident tracking. A MSHP official said this system was in development before the start of the audit.

Without an adequate method to report, track, and monitor potential incidents of inappropriate use of CJI, there is an increased risk that incidents may not be subject to management oversight and be appropriately investigated.

1.2 Security audits

MSHP management has not performed security audits of agencies with direct access to the MULES since July 2012, and not all agencies with direct access to the MULES received audits prior to that time. In addition, MSHP management has not documented the policies or fully established the procedures necessary to perform security audits.

A MSHP official said security audits have not been performed because the unit responsible for the audits was not established until 2010 and lacked sufficient staffing. This official said the MSHP submitted a risk assessment survey to agencies during 2014, and based on the assessment results, plans to begin performing security audits starting with the higher risk rated agencies. However, this official believes submitting risk assessment questionnaires to local agencies meets the minimum CJIS Security Policy audit requirements.

The CJIS Security Policy requires performing audits at least every 3 years of all agencies with direct access to the state system. Without conducting security audits, management is unable to effectively ensure agencies are in compliance with applicable statutes, regulations, and policies. In addition, MSHP management faces an increased risk that security weaknesses or control deficiencies are not detected that could compromise the confidentiality, integrity, and availability of CJI maintained by the MULES.

Federal auditors also reported issues regarding physical security inspections of local agencies.

1.3 Policy compliance reviews

MSHP management has not fully documented policies or established procedures for performing PCR audits of criminal justice agencies with direct access to the MULES or of agencies with access to CJI for noncriminal justice purposes.

Criminal justice agencies

According to the MSHP PCR manual, the objective of PCR audits are to assess agency compliance with the National Crime Information Center (NCIC) and MULES policies so agencies may continue to participate in the criminal justice information system. NCIC policy establishes a number of security measures to ensure the privacy, integrity, and quality of data. Both the NCIC and MULES policies require performing PCR audits every 3 years of agencies with direct access to the MULES, or that operate



Criminal Justice Information Security Management Management Advisory Report - State Auditor's Finding

workstations, access devices, mobile data terminals, or personal/laptop computers to access the MULES, to ensure compliance with state and CJIS Security Policy and regulations.

The NCIC requires PCRs to include procedures for ensuring (1) the accuracy, completeness, and timeliness of data entered into MULES (such as criminal history records); (2) an organization protects information against unauthorized access and ensures confidentiality of the information; and (3) information is released in accordance with applicable laws and regulations with a record of CJI dissemination maintained. During the PCRs, MSHP personnel also review compliance with other federal and state requirements, including whether appropriate agreements are in-place and compliance with background check and training requirements.

We tested 44 criminal justice agency PCRs performed by MSHP personnel during the period 2010 to 2014 and found:

- PCRs were not always performed timely. A PCR was not performed or not scheduled to be performed at least once every 3 years for 11 agencies. A MSHP official said this problem occurred due to the number of agencies the MSHP is required to audit and because the MSHP tries to reduce costs by scheduling audits of agencies in similar regions together. In addition, the MSHP became responsible for auditing an additional 265 agencies in 2011, requiring the 3 year audit cycle to be reset for 2013.
- Procedures performed during the PCRs were not always sufficiently documented. For example, MSHP personnel did not always document which agency users were selected for verifying compliance with background check and/or training requirements or why they did not review the minimum number of users, as dictated by MSHP policy. In addition, MSHP personnel did not sufficiently document why they did not perform additional reviews when agency users had limited or no criminal history record inquiries from the MULES during the time period selected.
- PCR documentation did not always contain evidence of appropriate review and approval. One of the 44 PCRs did not have documentation to support MSHP personnel reviewed and approved the PCR, but contained documentation supporting the peer review of the initial PCR and management review of the associated follow-up audit. In addition, seven PCRs did not have documentation to support an agency official reviewed and approved the PCR. A MSHP official said a programming error caused the electronic signature of the agency official to be unintentionally removed in certain instances. This official said this issue has now been corrected.



Criminal Justice Information Security Management Management Advisory Report - State Auditor's Finding

In addition, although MSHP management has developed a formal policy and procedure manual for performing the criminal justice agency PCRs, the manual has not been updated since 2012 and does not fully reflect current procedures.

Noncriminal justice agencies The CJIS Security Policy requires performing periodic audits of noncriminal justice agencies with access to CJI, and MSHP policy requires performing these PCR audits every 3 years. During these reviews, MSHP personnel verify compliance with applicable federal and state requirements, regulations and policies, such as ensuring appropriate agreements are in-place and proper dissemination of criminal history record information.

We selected 37 noncriminal justice agencies for testing the PCRs performed by MSHP personnel during the period of 2010 to 2013 and found:

- A PCR had not been performed for 21 agencies. A MSHP official said 11 of the 21 agencies had received CJI during the 3 year audit period so a PCR was necessary. This official said a PCR was subsequently performed for 7 of the 11 agencies after our audit inquiries. A MSHP official said a PCR was not performed for 10 of the 21 agencies because the MSHP had not submitted any CJI to these agencies during the 3 year audit period. However, sufficient documentation was not maintained on the audit tracking schedule to determine why the audits were not performed.
- PCR documentation did not always contain evidence of appropriate review and approval. For example, 13 PCRs did not have documentation to support MSHP personnel reviewed and approved the PCRs.
- The tracking system used for scheduling PCRs was not complete or effectively used. For example, the tracking system did not include all potential agencies required to be audited or a PCR audit was not always scheduled to be performed within 3 years of the prior audit or within a year of the agency being established. In addition, a MSHP official said periodic reconciliations have not been performed between the tracking system and the master list of noncriminal justice agencies to ensure the audit schedule includes all agencies that may require an audit. As a result, there is the risk a PCR audit may not be performed of an agency in accordance with policies or procedures.

Without effective monitoring and auditing procedures, MSHP management has less assurance agencies are in compliance with requirements and without adequate documentation to support the work performed and/or supervisory reviews of PCRs, there is an increased risk the PCRs will not be properly performed.



Criminal Justice Information Security Management Management Advisory Report - State Auditor's Finding

Noncompliance and subsequent action

MSHP management needs to improve controls and procedures for tracking and monitoring agencies that are not compliant with the minimum federal and state requirements.

MSHP management has not implemented a tracking system for documenting whether (1) the PCRs identified audit findings and noncompliance issues, (2) additional agency monitoring is planned or has been completed, and (3) disciplinary action has been taken. A MSHP official said the criminal justice audit results are not centrally tracked due to the significant number of PCR audits performed. However, without adequate tracking of PCR results and audit findings, there is an increased risk adequate follow-up may not occur. In addition, MSHP management does not have the information necessary for performing trend analyses of noncompliance issues and for identifying lessons learned that could be incorporated into security policies and practices.

MSHP management has not established adequate written guidelines regarding when follow-up monitoring reviews should be performed. MSHP policy states staff judgment is primarily relied upon to determine whether additional monitoring should occur when noncompliance with applicable statutes, regulations and policies is identified. Although decisions are made on a case-by-case basis, written guidelines would provide suggestions to help ensure subsequent actions are handled consistently. In addition, if follow-up monitoring is performed and the agency is still not in compliance, MSHP policy indicates the CSO may require the agency to provide a specific plan of action to address the deficiencies.

Of the 44 criminal justice agency PCRs reviewed, MSHP personnel identified a total of 150 noncompliant issues occurring in 34 agencies. Examples of noncompliance included agency users not meeting background check and training requirements, and potential inappropriate use of CJI. MSHP personnel performed follow-up reviews for 9 of the 34 criminal justice agencies, but did not document why follow-up reviews were not performed for the remaining 25 agencies. MSHP personnel found 5 of the 9 agencies still had 20 noncompliant issues outstanding.

MSHP personnel identified 16 noncompliant issues at 7 of the 16 noncriminal justice agencies that had a PCR performed. Examples of noncompliance included not destroying CJI records when no longer needed and not logging the dissemination of all CJI records. MSHP policy states a follow-up PCR will be performed when noncompliance with applicable statutes, regulations and policies is identified. However, MSHP personnel did not perform any additional follow-up monitoring to ensure these deficiencies were subsequently corrected.



Criminal Justice Information Security Management Management Advisory Report - State Auditor's Finding

Without effective procedures for tracking and monitoring agencies that are not compliant with minimum requirements, there is an increased risk these agencies will continue to be noncompliant with federal and state requirements. As a result, management is at risk of not being able to ensure the confidentiality, integrity, and availability of CJI.

1.4 Periodic background checks

MSHP management has not established procedures to ensure background reinvestigations of MSHP users with access to the MULES are performed. A MSHP official said background reinvestigations of MSHP personnel with direct access to CJI have not been performed. MSHP officials were not aware these reinvestigations had not been occurring until our audit inquiries.

MULES policy requires biennial background reinvestigations of MULES users. Without ensuring appropriate background reinvestigations are performed, there is an increased risk of exposing sensitive CJI or other information to an employee or user with an adverse background.

1.5 Agreements

MSHP management needs to improve controls and procedures to ensure agreements with agencies are properly executed and comply with federal and state requirements.

Agency user agreements

MSHP management has not entered into user agreements with some agencies that have access to CJI. The agreements include agency responsibilities, the forms and methods of acceptable use, penalties for violation, and disclaimers.

We tested 40 criminal justice agencies and 40 noncriminal justice agencies required to have agency user agreements with the MSHP. An agreement was not available for 5 of the criminal justice agencies and 7 of the noncriminal justice agencies. In addition, a MSHP official said 27 other criminal justice agencies did not have agency user agreements with the MSHP as of May 2014. A MSHP official said 1 of the criminal justice agencies was no longer an active agency and officials have requested the other 31 agencies to submit user agency agreements. While the MSHP does have authority to discontinue agency access for not submitting an agreement, an official said agency access remains in place due to safety issues and other concerns.

The CJIS Security Policy requires the CSA to establish written agency user agreements before agencies receive access to CJI or before CJI is exchanged. Without appropriate agreements in place, MSHP management does not have assurance all agencies are aware of and acknowledge program responsibilities.



Criminal Justice Information Security Management Management Advisory Report - State Auditor's Finding

Management control agreements

MSHP management has not ensured certain agencies have entered into management control agreements or adequately ensured agreements meet federal recommendations.

MSHP management entered into a management control agreement with a noncriminal justice agency performing certain information technology services for the MSHP; however the agreement was established in 2003 and did not include many provisions recommended by the CJIS Security Policy. MSHP management also entered into a memorandum of understanding with another noncriminal justice agency performing certain information technology services for the MSHP; however, the agreement did not include many provisions recommended by the CJIS Security Policy. Finally, the Regional Justice Information Services (REJIS),⁷ a noncriminal justice agency, has not entered into management control agreements with the criminal justice agencies it services. In March 2014, the MSHP and the REJIS finalized a management control agreement template for the REJIS agencies and the MSHP has been working to ensure compliance.

The CJIS Security Policy requires a noncriminal justice agency receiving access to CJIS to enter into a management control agreement with the criminal justice agency providing the access. The CJIS Security Policy requires management control agreements to stipulate management control of the criminal justice function remains solely with the criminal justice agency. Without appropriate agreements in place, MSHP management does not have assurance all agencies are aware of and acknowledge program responsibilities.

1.6 Training

MSHP management has not fully ensured users with access to CJIS receive adequate security awareness training or are sufficiently aware of security responsibilities. Security awareness includes notifying users of the importance of the information they handle, distributing documentation describing security policies and expected behavior, and requiring users to periodically sign a statement acknowledging their awareness and acceptance of responsibility of security, according to the GAO.

Criminal justice agencies

The CJIS Security, NCIC, and MULES policies all require personnel with physical and logical access to CJIS to attend security awareness training within 6 months of initial assignment and biennially thereafter. In addition, the MULES policy requires all MULES users to attend a certification course

⁷ REJIS is a quasi-government entity created to provide information technology products and services to criminal justice and government agencies. REJIS has about 265 criminal justice and government customers. REJIS was previously considered a Regional Criminal Justice Agency, but during calendar year 2011, the FBI removed this authorization and required the REJIS to report to the MSHP. At this time, the MSHP became responsible for ensuring compliance by REJIS and the criminal justice agencies it services.



Criminal Justice Information Security Management Management Advisory Report - State Auditor's Finding

within 6 months of initial assignment and biennially thereafter. This certification includes several modules, such as how to correctly and accurately enter CJI into the MULES. The NCIC policy also requires appropriate training on effective use of the system. We identified the following risks and noncompliance with applicable training policies:

- ICTD and MSHP contractor personnel are not required to attend certification training prior to being granted access to the MULES or biennially thereafter. A MSHP official said these users were not required to attend training because they were not responsible for modifying any data in the system. However, MSHP officials said the MSHP is working to correct this issue.
- MSHP management has not required and/or ensured personnel at certain state agencies attend security awareness training prior to being granted access to CJI or biennially thereafter. A similar condition was previously reported by federal auditors.

Dissemination and enforcement of policies are critical as employees cannot be expected to follow policies for which they are not informed, according to accepted standards. Without adequate training, users may not understand system security risks and their role in implementing related policies and controls to mitigate those risks, according to the GAO.

Noncriminal justice agencies

In August 2013, the MSHP developed a security awareness training course for personnel at noncriminal justice agencies to attend; however, a MSHP official said most agencies had not been notified of this course. As a result, this official said most agency personnel have not participated in the security awareness training provided by the MSHP. The CJIS Security Policy requires all personnel at agencies with access to CJI for a noncriminal justice purpose to attend security awareness training. A MSHP official also said monitoring or follow-up has not been performed to ensure personnel at these agencies received security awareness training. In addition, personnel at noncriminal justice agencies are not required to sign a statement acknowledging awareness and acceptance of responsibility of security nor are these personnel provided rules of behavior notifications prior to being granted access to the CJI.

Effective security-related personnel policies are critical to effective security, according to the GAO. Ineffective personnel policies can result in personnel or contractors inadvertently or intentionally compromising security.



Criminal Justice Information Security Management Management Advisory Report - State Auditor's Finding

Recommendations

The MSHP:

- 1.1 Establish criteria for unusual and inappropriate activity then monitor and review the audit trail logs to identify improper access, use, or dissemination of CJI. In addition, ensure procedures for reporting, tracking, and handling potential cases of misuse of CJI are fully established and documented.
- 1.2 Document the policies and procedures for performing security audits, and ensure such audits are performed within timeframes required by federal policy.
- 1.3 Update the PCR manual, and review and perform PCRs in compliance with federal and state requirements. In addition, the MSHP should establish adequate controls and procedures for tracking and monitoring noncompliant agencies.
- 1.4 Ensure periodic background checks are performed.
- 1.5 Establish procedures to ensure appropriate agreements are in-place, current, and meet recommendations for agencies receiving access to CJI.
- 1.6 Ensure users with access to CJI are sufficiently trained and aware of their security responsibilities in accordance with federal and state requirements.

Auditee's Response

- 1.1 *Continuous efforts are currently made to detect, prevent and deter instance of misuse of CJI. The regulation over the use, and protection of CJI is managed through a shared management philosophy as outlined in CJIS Security Policy Version 5.3 in section 3.2. Through this shared management approach, it is incumbent that local jurisdictions bear some responsibility for monitoring system activity and detecting misuse. The MSHP continues to improve internal procedures to ensure that as the state CSA we are constantly working to deter, detect and respond to instance of misuse of official information. Recently, this work has included developing enhanced reporting capabilities to better track reported instances of misuse as well as requiring local jurisdictions report instances of misuse or improper access to the MSHP within 24 hours of discovery.*
- 1.2 *A security audit program has been developed and security audits of local agencies are currently underway. This program falls under the direction of the MSHP Information Security Unit (ISU), which continues to develop since its creation in 2010.*



Criminal Justice Information Security Management Management Advisory Report - State Auditor's Finding

- 1.3 *As the designated CJIS CSA for Missouri, the MSHP has conducted 2,518 CJIS PCRs of criminal and noncriminal justice agencies since the beginning of 2011. With more than 250 REJIS agencies now fully incorporated into the MSHP's 2013-2015 and 2016-2018 CJIS audit cycles, all 792 Missouri criminal justice agencies accessing the NCIC/MULES systems will be audited once every 3 years. Additionally, the MSHP has already begun updating the 120 page MULES PCR manual to reflect 2015 policy. Finally, by allocating funds to purchase new software specifically designed to manage NCIC, National Data Exchange (N-DEx), Civil, and Uniform Crime Reporting audits, the MSHP CJIS Division will be able to create a more mobile web-based audit document, track all operators and noncompliant agencies in greater detail, and instantly analyze the data retrieved from over 600 audits conducted by MSHP personnel each year.*
- 1.4 *As a part of the implementation of the MSHP's information security strategic plan, the responsibility for performing biennial re-investigations of MSHP personnel has been shifted to the ISU. All MSHP personnel undergo a complete pre-employment background investigation and are mandated by internal policy to report any arrests or citations to their commanding officer. The process for performing biennial investigations is being developed and formally documented. Upon its completion, the re-investigation process will begin on all employees having served with the MSHP for more than 2 years.*
- 1.5 *The MSHP maintains thousands of various agreements with agencies accessing systems that contain CJI. A process had already been implemented prior to this audit that requires any new agency requesting access to protected systems or data to execute an agreement before any access is granted. As policy requirements frequently change, the process of obtaining new agreements for each existing agency is continuous. While the MSHP has the regulatory authority to discontinue access to systems and data in the event an agency fails to sign an agreement, exercising such authority could have a very detrimental effect on public safety. The impact of such a decision may result in a school district not being able to appropriately perform background checks on prospective school teachers or local law enforcement not being able to inquire on the status of a possible stolen vehicle or wanted person. With these serious considerations in the balance, the MSHP has historically elected to err on the side of public safety and continuously work with agencies to execute agreements in lieu of punitive actions.*



Criminal Justice Information Security Management Management Advisory Report - State Auditor's Finding

1.6 *The MSHP will continue its extensive efforts in the area of MULES training. These efforts will include ensuring the 63 users requiring additional training, (representing less than one percent of the 21,169 MULES users statewide) receive the required training as cited in this audit.*

2. User Account Management

MSHP management has not fully established and documented user account management policies and procedures. In addition, policies and procedures for the management of privileged user accounts or users with significant access⁸ has not been fully established. User account management includes requesting, establishing, issuing, suspending, modifying, closing, and periodically reviewing user accounts and related user privileges, according to accepted standards. User account management policies and procedures should be established for all user accounts, including system administrators.

2.1 Account access policies

MSHP management has not fully established policies and procedures for requesting, granting, and removing access to the network, the MULES, or supporting systems.

The access authorization process for privileged user access to the network, MULES, or other supporting systems has not been standardized and source documentation to support access approval was not always retained. A MSHP official said in some cases the individuals with privileged access have been employed for so long there probably would not be any documentation maintained to support access. In addition, the process for requesting, authorizing, and removing terminal accounts or license keys has not been formally established. A terminal account and license key are used, in conjunction with a user account, to control and secure access to the MULES. A MSHP official said terminal account and license key requests are generally received in an email from local agencies.

MSHP management has not fully established procedures to ensure access request documents are maintained; properly approved; or completely and accurately entered into the system responsible for maintaining and tracking user access requests. We identified the following risks:

- Manual access requests forms required to support user access were not always maintained, properly approved, or did not contain some required information. We tested 22 user accounts and identified manual access request forms (1) were not on-file for 2 accounts; (2) were not formally approved for 2 accounts; and (3) did not contain necessary information,

⁸ Privileged users are individuals who have access to system control, monitoring, or administration functions (such as system administrator). Users with significant access have the ability to perform most functions within the network or MULES or other supporting systems.



Criminal Justice Information Security Management Management Advisory Report - State Auditor's Finding

such as a user signature or that training was verified, for 8 accounts. The accounts for 7 of the 12 problems identified were established prior to 2012, which was before the MSHP implemented new request form processing procedures.

- Access requests for certain users are not entered into the system responsible for maintaining and tracking access requests. As a result, MSHP management does not have a complete audit trail to document who processed the access or removal request. A separate process has been established for these users; however, a MSHP official agreed there is no audit trail documenting who processed these requests.
- The access request system does not have controls requiring entry of certain data fields, such as who approved the access request. As a result, there is an increased risk a user could be granted access to the MULES without appropriate approval. A MSHP official said the information is typically entered in the system; however, there is no system edit requiring completion of this information.

CJIS Security Policy states agencies shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. A formal process for transmitting access authorizations, including the use of standardized access request forms, should be established to reduce the risk of mishandling, alterations, and misunderstandings, according to the GAO. Without appropriate account access policies, users may be granted inappropriate or unauthorized access, which can provide opportunities for inappropriate disclosures.

2.2 Periodic review of user accounts

MSHP management has not fully established procedures for administering and reviewing user access to data and other information resources on the network, MULES, or supporting systems to ensure access rights are commensurate with job responsibilities and remain appropriate.

The CJIS Security Policy requires the MSHP to validate information system accounts at least annually and to document the validation process. The validation and documentation of accounts can be delegated by the MSHP to local agencies. In addition, MSHP policy requires an annual validation of access authorizations for MSHP personnel. Accepted standards also support regular review of all accounts and related privileges. At a minimum this review should include levels of authorized access for each user, whether all accounts are still active, and whether management authorizations are up-to-date, according to accepted standards. Without a review of user access rights, there is an increased risk that unauthorized alterations of these rights would go undetected or that access rights would not be aligned with current job duties.



Criminal Justice Information Security Management Management Advisory Report - State Auditor's Finding

Review of accounts to determine inappropriate access

MSHP management has not fully established procedures for periodic reviews of accounts and related privileges.

MSHP management has not periodically provided a list of user accounts for information technology support personnel with access to the network or certain other systems supporting the MULES to appropriate agency personnel for review. In addition, procedures have not been established to periodically provide a list of MULES terminal accounts to appropriate agency personnel for review. Without a complete list of all accounts, management cannot review or confirm user access rights are appropriate.

MSHP management conducted an annual review of MULES users in August 2013. However, sufficient documentation was not maintained to support the review. For example, MSHP personnel did not (1) maintain a complete list of agencies required to perform user validations, (2) fully track whether validations were returned, (3) maintain documentation to support validations of certain privileged users were performed, or (4) ensure validations were received timely. A MSHP official said procedures for tracking and documenting the agency user reviews were improved for the August 2014 annual validation. If procedures are fully established, MSHP management will have the capability to more effectively manage information system accounts and to reduce the risk of inappropriate access to CJI.

Both the CJIS Security and the MSHP policies require the MSHP to validate information system accounts at least annually. Requiring a review of all accounts ensures the right type and level of access has been provided. Otherwise, user accounts and accesses can be granted to or maintained for users who should not have access, according to accepted standards.

Inactive user accounts

MSHP management has not performed timely, periodic reviews to identify user and terminal accounts that have not been accessed or used for a specified period of time for either the network or the MULES.

This weakness occurred, in part, because the MULES does not have the functionality to fully record the last date a user or terminal account was accessed. For example, the MULES does not record the last date a user account accessed the MULES remotely rather than directly (see MAR finding number 2.6). A MSHP official said the last use date may also not accurately record the last time a user performed a transaction, such as an inquiry, but instead records the last time a security function was performed on a user account. In addition, MSHP management allows certain accounts to have the last login date set to not expire, in which case the MULES does not record the last date a user account accessed the MULES.



Criminal Justice Information Security Management Management Advisory Report - State Auditor's Finding

As noted in the following table, 13,587 (64 percent) of the 21,169 user accounts had a non-expiring last use date or had not been accessed since 2013 or before, according to MULES user account records.

Age of Last Login to the MULES by
Active MULES User Accounts¹

Year of Last Login	Number of Accounts	Cumulative Number of Accounts	Cumulative Percent of Total
Non-expiring ²	1,764	1,764	.08
2012	9,012	10,776	50.90
2013	2,811	13,587	64.18
2014	7,582	21,169	100.00
Total	21,169		

¹ The current MULES security system was established in 2012. Last login data is as of November 2014.

² A MSHP official said some accounts set to not expire were not appropriate.

A MSHP official said periodic reviews to identify inactive accounts are not performed because (1) agencies are responsible for notifying the MSHP if a user no longer needs access, (2) the user account will not be able to access the MULES if the user has not attended training within a period of time, (3) the password controls help prevent inappropriate users from accessing the MULES, and (4) the annual review of MULES users assists in reducing unauthorized access. A MSHP official said the MSHP has requested the contractor responsible for the MULES to establish functionality to fully record the last date a user or terminal account was accessed.

Without appropriate security control functionality, MSHP management is unable to identify user accounts that had not been accessed or used for a specified period of time. Inactive accounts indicate users no longer need the access privileges provided by the accounts and may be attractive targets for individuals attempting to gain unauthorized access since the account owners may not notice illicit activity on the accounts, according to the GAO.

Tracking user account
information

MSHP management has not ensured internal databases that maintain user account information are periodically reconciled to network or MULES user accounts. Internal databases are used to store and track information about user accounts, including access requests and are an important component for maintaining security. These databases do not interface with the network or the MULES and must be updated by MSHP personnel to reflect information from several data sources, including access request forms. However, a MSHP official said reconciliations between these internal databases and the network or the MULES are not performed. Without performing periodic reconciliations, there is an increased risk of data integrity issues between information sources and an increased risk of inappropriate access to system resources.



Criminal Justice Information Security Management Management Advisory Report - State Auditor's Finding

2.3 Termination of user accounts

As of November 2014, twenty former MSHP employees still had access to the MULES, potentially including access to CJI. One former employee left MSHP employment in May 2013, while the remaining 19 left employment between January and October 2014. This problem occurred, in part, because MSHP management has not fully established policies and procedures to perform periodic reviews to identify terminated or transferred users with access to the network or the MULES. The CJIS Security Policy requires an agency, upon termination of employment, to immediately remove an individual's access to CJI. In addition, MSHP policies and procedures require supervisors or human resource staff to notify MSHP staff of employees that have left employment. MSHP staff are then responsible for disabling the user account. However, MSHP staff do not perform periodic reconciliations to the state human resource system to identify terminated or transferred employees with active access to the MULES or network, according to a MSHP official.

Without effective procedures to remove access upon termination or an acrimonious circumstance, terminated employees could continue to have access to critical or sensitive resources or opportunities to sabotage or otherwise impair entity operations or assets, according to the GAO.

2.4 Removal of accounts

MSHP management has not established procedures to review user and terminal accounts that have been disabled for extended periods of time to determine whether these accounts can be permanently removed. As of November 2014, MSHP officials maintained 13,020 disabled MULES user accounts. The majority of these accounts still had associated access rights to perform functions within the MULES should the account be re-enabled.

One of the most effective ways to prevent unauthorized access to a system is to eliminate unnecessary accounts. While disabling accounts that are no longer needed is a good practice and may be necessary to maintain audit trails to comply with regulations, without periodically reviewing and removing disabled accounts there is an increased risk of an account being accidentally or deliberately re-enabled resulting in inappropriate access.

2.5 Privileged user supervision

MSHP management did not require supervisory reviews of system logged actions performed by privileged users or other users with significant access to the network, MULES, or other supporting systems.

Although MSHP management has generally properly segregated computer and system functions, we identified instances where duties were not properly segregated and additional supervisory reviews were not performed. For example, certain computer operations personnel with privileged access to the MULES have the ability to perform system administration and security administration functions. To illustrate, the individuals responsible



Criminal Justice Information Security Management Management Advisory Report - State Auditor's Finding

for performing system support were also responsible for adding and deleting system users, and software change management functions.

Privileged users have extensive access rights necessary to keep systems running efficiently. Sometimes these job duties are difficult to segregate due to staffing or other issues. Even when proper segregation has been established, the actions of privileged users warrant supervision due to the extensive rights these users are provided. However, MSHP management did not provide supervisory oversight or establish other mitigating controls to ensure these privileged users performed only authorized functions. Changes made by privileged users or users with significant access to the MULES are logged, but a MSHP official said the logs are not reviewed regularly.

Routinely monitoring security administrator actions can help identify significant problems and deter employees from inappropriate activities. Without effective monitoring, an increased risk exists that these individuals could perform unauthorized system activities without being detected.

2.6 System functionality

The MULES does not have the functionality to maintain a complete and accurate audit trail of security events for users accessing the MULES using remote access devices. Maintaining an audit trail of security events is necessary to perform user account administration and ensure compliance with the CJIS Security Policy.

At least 56 percent of the active MULES user accounts have the ability to access the MULES using remote access devices. Due to limitations in MULES functionality, these users are not required to follow certain centralized security controls required of users accessing the MULES directly. Instead, the MSHP relies on the local agencies to ensure access security controls are proper, secure, and in compliance with requirements. We identified the following risks:

- Users accessing the MULES using remote access devices are not required to comply with centralized MULES password controls. According to MULES user account information, 14,236 of the 21,169 (67 percent) active user accounts had an expired password as of October 31, 2014. Password controls for remote access users are generally established at the local agency level.
- MSHP management is unable to identify the last date a remote user accessed MULES.
- Users accessing the MULES using remote access devices are not required to comply with the MULES concurrent session setting controls.

Without system functionality to maintain a complete and accurate audit trail of security events for users accessing the MULES using remote access



Criminal Justice Information Security Management Management Advisory Report - State Auditor's Finding

devices, management may not be able to ensure the confidentiality, integrity, and availability of data and the system. This risk could be minimized by performing security audits to identify if local agencies have established effective procedures to ensure security controls are proper, effective, and in compliance with requirements. However, the MSHP has not been performing security audits of agencies with access to the MULES (see MAR finding number 1.2).

2.7 Access rights and privileges

MSHP management has not fully documented access profiles⁹ that may be assigned to MULES users. Access rights and privileges are used to determine what a user can do after being allowed into the system (such as read or write to a certain file or directory), according to the GAO. A MSHP official said access profiles are routinely added and modified and documentation is currently being revised.

Without adequate documentation, user access profiles may not be effectively communicated to both administrators and supervisors responsible for granting access and management cannot ensure access has been appropriately granted to only authorized individuals.

Recommendations

The MSHP:

- 2.1 Establish and document policies and procedures for requesting, granting, and approving access to the network, MULES, and other supporting systems.
- 2.2 Periodically review user access to data and other information resources to (1) ensure access rights are commensurate with job duties and responsibilities, (2) identify and evaluate inactive accounts, and (3) periodically reconcile user account information maintained in internal databases to account information from the network or the MULES.
- 2.3 Implement procedures to ensure user accounts and related access privileges are removed timely upon employee termination.
- 2.4 Implement procedures to periodically review and remove disabled user accounts.
- 2.5 Perform periodic supervisory reviews of defined actions performed by privileged users or users with significant access.

⁹ Profiles are the various privileges or roles available within each application, such as access to CJI or driver's license records and their respective rights, such as read-only, update, administrator, etc.



Criminal Justice Information Security Management Management Advisory Report - State Auditor's Finding

- 2.6 Evaluate establishing functionality in the MULES to ensure a complete and accurate audit trail of security events is maintained and recorded for users accessing the MULES using remote access devices. If enhanced functionality is prohibitive, establish effective compensating controls to help ensure MULES security.
- 2.7 Complete the process of documenting user access profiles.

Auditee's Response

- 2.1 *While there is always room for improvement, policies and procedures currently exist controlling access to various MSHP managed systems. Through the implementation of the MSHP's information security strategic plan, existing policies and procedures are being reviewed and revised as appropriate. Additionally, all access control functions have recently been reassigned to the MSHP ISU under the direct supervision of the MSHP Chief Information Security Officer (CISO). This change ensures proper separation of duties between system administration and security administration functions.*
- 2.2 *The MSHP currently validates all MULES user accounts annually. The internal account review process is currently being reviewed and adjusted to accommodate the move to a more comprehensive identity and access management control model.*
- 2.3 *Timely user account access termination is now being addressed through better coordination between the human resources division and the information security unit.*
- 2.4 *The MSHP currently maintains all inactive accounts in disabled status to ensure accurate audit logs and to comply with regulatory and legal requirements. Direct oversight by the MSHP ISU ensures these accounts are maintained in a secure state and any risk associated with storage is properly mitigated.*
- 2.5 *Through the implementation of the MSHP's information security strategic plan, the ISU is currently enhancing its capabilities to monitor privileged user actions, reporting anomalies and suspicious behavior to the CISO.*
- 2.6 *The MSHP will continue to ensure that users/devices of REJIS and other third-party remote systems authenticate against the state's central user/device directory to facilitate enhanced security controls and logging.*
- 2.7 *The MSHP currently maintains a comprehensive user access profile definition document. This document did not contain the level of*



Criminal Justice Information Security Management Management Advisory Report - State Auditor's Finding

detail desired by the State Auditor's office (SAO) at the beginning of the audit process. This document has since been updated to meet all of the SAO's requirements.

3. Information Security Program

While MSHP management has made several significant improvements to the information security program since 2012, opportunities exist to strengthen the program and to improve the protection of information system resources.

MSHP management has not fully implemented certain elements of an information security program on which security plans, policies, procedures, and controls can be formulated, implemented, and monitored. Although management is committed to and has taken significant steps to develop an information security program, weaknesses exist that threaten the confidentiality, integrity, and availability of MSHP information and systems.

An information security program provides a framework for managing risks, developing security policies, assigning responsibilities, and monitoring the adequacy of an agency's security controls. An information security program is the foundation of an agency's security control structure and a reflection of management's commitment to addressing security risks. Implementing a security program is essential to ensuring controls over information and information systems work effectively on a continuing basis, according to the GAO.

MSHP management has not fully established and/or documented policies and procedures for the following elements of an information security program:

- Risk assessment
- Incident response plan
- Security activity logging and review
- Password policies
- Unsuccessful login attempts
- Review of security settings
- Physical security
- Protection of electronic media in transport
- Media sanitization and destruction
- Responsibilities of those accountable for security
- Review of key standards and policies

According to accepted standards, policies are necessary to set organizational strategic directions for security and assign resources for implementation of security. A key element of an effective information security program is to develop, document, and implement risk-based policies and procedures that



Criminal Justice Information Security Management Management Advisory Report - State Auditor's Finding

govern the security over an agency's computing environment, according to the GAO.

3.1 Risk assessment

MSHP management has not established a comprehensive risk assessment and management program.

Accepted standards state organizations should develop, document, and implement an information security program that includes periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems. A risk assessment is necessary to identify potential threats, identify vulnerabilities in systems, determine the likelihood that a particular threat may exploit vulnerabilities, and assessing the resulting impact on the organization's mission, including the effect on sensitive and critical systems and data, according to accepted standards. Risk assessments should include essential elements such as discussion of threats, vulnerabilities, impact, risk model, and likelihood of occurrence, and be updated using the results from ongoing monitoring of risk factors. MSHP officials acknowledge that, while portions of a risk assessment are in place, the assessment is not complete or comprehensive, and a revised risk assessment is being prepared.

Without an established risk management and assessment framework in place, unidentified risks or threats may expose an unknown system vulnerability; resulting in lost information, lost privacy, loss of availability, or loss of system integrity. In addition, MSHP management has less assurance that established security controls are cost-effectively addressing programmatic risks.

3.2 Incident response plan

MSHP management has not fully established an incident response plan. Incident handling and response is the process and actions an organization takes in detecting, reporting, and responding to a computer security incident, according to accepted standards. Once an incident has been identified, an agency's incident response procedures should provide the capability to correctly log the incident, properly analyze it, and take appropriate action, according to the GAO.

Examples of procedures required by the CJIS Security policy or recommended by accepted standards that have not been effectively established or documented include:

- Roles and responsibilities of those responsible for incident handling.
- Prioritization of incidents, including timeframes for resolving incidents.
- Collection of incident evidence.
- Containment, eradication, and recovery strategies.
- Lessons learned, including metrics to measure the incident response capability and its effectiveness.



Criminal Justice Information Security Management Management Advisory Report - State Auditor's Finding

The CJIS Security Policy requires agencies to document and track information system security incidents on an ongoing basis and to maintain completed security incident reporting forms. However, a MSHP official said prior to our audit inquiries, the MSHP did not have a centralized mechanism to record and track security incidents, but the MSHP was currently implementing a new incident reporting system.

Without effective incident handling policies and procedures, an agency may be hampered in its ability to detect incidents, report incidents to the appropriate authorities, minimize the resultant loss and destruction, mitigate the exploited weaknesses, and restore services, according to the GAO.

3.3 Security activity logging and review

MSHP management has not fully ensured audit trail records for defined security and audit related events are produced or reviewed. Determining what, when, and by whom specific actions were taken on a system is crucial to establishing individual accountability, monitoring compliance with security policies, and investigating security violations, according to the GAO.

MSHP management has not defined the security events to be logged and reviewed. The CJIS Security Policy requires agencies to maintain and periodically review and update the list of agency-defined auditable events. A MSHP official said since all activity is logged, the MSHP is technically in compliance with CJIS requirements. However, policies and procedures should establish the criteria for significant system events that should be logged and independently reviewed by management, according to accepted standards.

In addition, the MULES does not have the capability to log user account additions, changes, or deletions, according to a MSHP official. As a result, MSHP management is unable to effectively determine when a user account was added, disabled, or removed from the system. The CJIS Security Policy requires the agency's information system to produce audit records for defined security events, and contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. For example, the CJIS Security Policy requires that certain significant events be logged including successful and unsuccessful attempts to create, change, or delete user accounts; change passwords; or modify the audit log file.

How agencies configure the system or security software determines the nature and extent of audit trail information that is provided, according to the GAO. To be effective, agencies should (1) configure the system to collect and maintain sufficient audit trails for security-related events; (2) generate reports that selectively identify unauthorized, unusual, and sensitive access activity; and (3) regularly monitor and take action on these reports. Without



Criminal Justice Information Security Management Management Advisory Report - State Auditor's Finding

sufficient auditing and monitoring, organizations increase the risk that they may not detect unauthorized activities or policy violations.

3.4 Password policies

MSHP management has not consistently ensured all users are uniquely identified, that passwords are not shared and are changed every 90 days, or reported timely if the password is lost or compromised. We identified the following risks and noncompliance with applicable policies:

- The account and password for a MULES service level account is shared among several users and the password has not been periodically changed.
- The user identifications for certain accounts, such as network service accounts, are shared and/or the passwords are not set to expire. We identified that passwords are set not to expire for 1,956 of the 21,169 (9 percent) active MULES user accounts.
- New user accounts and passwords may be known by more than one individual. A MSHP official said when a new MULES user account is established, an agency official is notified of the new account through the terminal message notification system. The agency official then provides the account and password to the user. The user is not directly notified of the establishment of his/her user account and password. As a result, the password is at least initially known by more than one individual.

Both the CJIS Security and MULES policies contain provisions for protecting user identifications and passwords. For example, users are required to be uniquely identified before performing actions on the system and users are responsible for protecting login information, including passwords, from use by others. In addition, the CJIS Security Policy requires passwords to be changed at least every 90 days and for users to immediately report lost or compromised passwords. Without strong password controls, the likelihood that accounts could be compromised and used by unauthorized individuals to gain access to sensitive information is increased, according to the GAO. By allowing users to share accounts and passwords, individual accountability for system activity could be lost and unauthorized system activity could occur.

3.5 Unsuccessful login attempts

The MULES does not have controls to limit the number of consecutive unsuccessful access attempts. Both the CJIS Security and MULES policies require user accounts to be locked for a period of time after a certain number of consecutive invalid access attempts. According to a MSHP official, the controls to lock a user account after a certain number of invalid access attempts was inadvertently omitted when the MULES was upgraded in the fall of 2012.



Criminal Justice Information Security Management Management Advisory Report - State Auditor's Finding

Without effective controls to limit the number of consecutive unsuccessful access attempts, there is less assurance CJI is effectively protected from unauthorized access.

3.6 Review of security settings

MSHP management has not established formal written policies to periodically review and evaluate the effectiveness of security settings for the MULES or the network. Although policies have not been established to require periodically reviewing security settings, a MSHP official said security settings are reviewed and tested before changes to the MULES or network are implemented. According to the GAO, a key element of a security management program is ongoing testing and evaluation to ensure systems are in compliance with policies, and that policies and controls are both appropriate and effective.

3.7 Physical security

MSHP management has not fully established or documented the physical security policies and procedures necessary to ensure MSHP computer resources are properly controlled, monitored, and restricted to only authorized individuals. Physical security controls should be designed to prevent vandalism and sabotage, theft, accidental or deliberate alteration or destruction of information or property, attacks on personnel, and unauthorized access to computing resources, according to the GAO. Inadequate physical security could lead to the loss of property, the disruption of service and functions, and the unauthorized disclosure of documents and information.

User access policies and procedures

MSHP management has not established policies and procedures for requesting, granting, and removing physical access to areas housing information technology resources. MSHP officials said a method to request and approve access authorizations or terminations has not been standardized and access request and approval source documentation has not been retained.

The CJIS Security Policy requires that physical protection policies and procedures be documented and implemented to ensure CJI are physically protected through access control measures. Management should define and implement procedures to grant, limit and revoke access to premises, buildings, and areas according to business needs, including emergencies, according to accepted standards. Without appropriate procedures to grant and remove access to sensitive areas, individuals may be granted inappropriate or unauthorized access.

Review of user access

MSHP management has not fully established procedures for reviewing access to the server room to ensure access rights are commensurate with job responsibilities.



Criminal Justice Information Security Management Management Advisory Report - State Auditor's Finding

We found management had not maintained adequate documentation to support when the last user access review was performed or the results of the review. We reviewed both a report of users with access to the server room created by MSHP management and a system-generated report and found differences between the reports. According to a MSHP official, five MSHP employees had inappropriate access based on current job responsibilities and were removed from the MSHP created report prior to providing the information to us.

Agencies should periodically review the physical access granted to computer facilities and resources to ensure the access continues to be appropriate, according to the GAO. Without a formal documented review, physical access may be granted to or maintained for individuals who should not have access.

Review of access logs

MSHP management has not fully established procedures to identify unusual or inappropriate activity by performing periodic reviews of the server room door access logs.

A MSHP official said procedures have not been established to monitor the server room door activity logs. We reviewed the server room access activity logs for a 6-month period and found:

- Eight instances where server room access was denied, but the alarm notification records were not reviewed timely.
- Two instances where the door to the server room was open too long and the alarm notification records were not reviewed timely.
- One instance where the alarm notification record was not reviewed by an independent individual.

The CJIS Security Policy requires agencies to monitor physical access to the information system to detect and respond to physical security incidents. Reviewing security logs is necessary to identify apparent security violations or suspicious physical access activities, such as access outside of normal work hours or access for unusual lengths of time, according to accepted standards. Without a periodic review of the server room activity logs, management may not detect unusual or inappropriate activity.

3.8 Protection of electronic media in transport

MSHP management has not fully established controls to protect electronic media containing CJIS while in transport (data is physically moved from one location to another) to help ensure the confidentiality and integrity of the data. Encryption is a control used to ensure the confidentiality, integrity, and availability of sensitive data during storage and transmission and reduces the risk that unauthorized users could access the data, according to the GAO.



Criminal Justice Information Security Management Management Advisory Report - State Auditor's Finding

According to the CJIS Security Policy, encryption is the best control during data transport. However, if encryption is not possible then an agency should implement other controls to ensure the security of the data. A MSHP official said the data on certain electronic devices are protected and the MSHP is exploring options to ensure all electronic media containing CJIs are adequately protected during transport. Without encryption controls, sensitive data or resources may not be adequately protected from unauthorized access and improper disclosure.

A similar condition has been previously reported by federal auditors.

3.9 Media sanitization and destruction

MSHP management has not fully established or documented policies and procedures for the sanitization and destruction of electronic media containing CJIs.

Although MSHP management has established a sanitization and destruction policy, the policy is not a formally approved agency-wide order. As a result, there is the risk not all MSHP personnel are aware of the policy. We also found the policy does not include some information recommended by accepted standards, such as (1) how media should be sanitized, (2) the sanitization method that should be used, (3) when media should be sanitized versus destroyed, and (4) the verification procedures that should be performed to ensure the media was properly sanitized or destroyed. In addition, MSHP management does not require or maintain adequate documentation to support an independent or supervisory review was performed to ensure media was properly sanitized or destroyed.

The CJIS Security Policy requires electronic media be properly sanitized prior to disposal or release for reuse by individuals not authorized to access CJIs; written documentation be maintained to support the steps taken to sanitize or destroy electronic media; and authorized personnel to ensure the electronic media are properly sanitized or destroyed. Effective sanitation and destruction policies and procedures are needed to ensure sensitive or confidential data is appropriately safeguarded and removed before the surplus, sale, transfer, or disposal of computer equipment. Without effective policies and procedures, sensitive data, may not be effectively protected from unauthorized disclosure.

3.10 Responsibilities of those accountable for security

MSHP management has not fully documented the roles and responsibilities and/or updated job descriptions for:

- Senior management or officials charged with establishing the department information security policy.
- Data and system resource owners responsible for making decisions regarding data classification and access rights to the MULES.



Criminal Justice Information Security Management Management Advisory Report - State Auditor's Finding

- Information security management responsible for providing and implementing information security controls, including physical security.
- System users with access to view, input, update, or modify the data stored within the MULES.

Without fully developing and documenting responsibilities, management may not have assurance that personnel with significant security roles are fully aware of their roles and responsibilities to protect the confidentiality, integrity, and availability of information and information systems to which they are assigned.

3.11 Review of key standards and policies

MSHP management has not fully established procedures for periodically reviewing and re-approving key standards, directives, policies, or procedures related to information technology and security. MSHP policy requires management personnel perform periodic reviews of policies to ensure continued compliance, necessity, and/or applicability of each directive. However, we found some policies have not been documented or are not in accordance with or reflective of current procedures. Without adequate reviews of key standards and policies, management cannot be assured system, technological, or organizational environments are adequately addressed.

Recommendations

The MSHP:

- 3.1 Establish a comprehensive risk assessment and management framework.
- 3.2 Establish and document an incident response plan that includes centrally tracking all security incidents.
- 3.3 Determine security events that should be logged and reviewed and fully ensure audit trail records for defined security and audit related events are produced and reviewed.
- 3.4 Strengthen password controls to reduce the risk of password compromise and to help prevent unauthorized access to CJI.
- 3.5 Establish controls to ensure user accounts are locked after multiple unsuccessful access attempts.
- 3.6 Develop formal policies to periodically review and test security settings.
- 3.7 Establish and document physical access policies and procedures for (1) requesting, granting, and removing access to the server room, (2) conducting and documenting periodic reviews of physical access



Criminal Justice Information Security Management Management Advisory Report - State Auditor's Finding

to ensure access rights are commensurate with job responsibilities, and (3) monitoring and reviewing server room door access logs on a periodic basis to identify unusual or inappropriate activity.

- 3.8 Require encryption of CJI in transport or implement other controls to ensure data security if encryption is not possible.
- 3.9 Fully establish and document policies and procedures for the sanitization and destruction of electronic media containing CJI.
- 3.10 Document the roles and responsibilities and update job descriptions of those responsible for information security.
- 3.11 Periodically review and re-approve key standards, directives, and policies and procedures.

Auditee's Response

- 3.1 *The MSHP implemented an official information security strategic plan in the fall of 2014 and was updated once again in January of 2015. This document was in development prior to the start of this audit and includes the formal establishment of an information security management framework as well as a call for a comprehensive risk assessment. An initial risk assessment has been completed by the ISU and a more in-depth review is currently underway.*
- 3.2 *The MSHP's incident response plan is currently under revision by the ISU. Prior to the start of this audit, development was already underway on a central security incident reporting and tracking system. This system, accessible by all MSHP employees and MULES users, was placed into production during the course of this audit.*
- 3.3 *As indicated in the SAO's findings, the MSHP currently logs all system events occurring across the enterprise environment. The information security unit is working to improve monitoring capabilities and response to audit log incidents.*
- 3.4 *Currently, the MSHP utilizes multiple controls to ensure password strength and complexity as well as several advanced authentication controls. Of the three issues identified in this audit, one has already been corrected and the remaining two are currently under review. The 9 percent of users erroneously provided with non-expiring passwords has been resolved.*
- 3.5 *The MSHP is currently working with a third-party vendor to address this recommendation.*



Criminal Justice Information Security Management Management Advisory Report - State Auditor's Finding

- 3.6 *All MULES security settings are tested when system changes are made. While this was not previously formally documented, policies and procedures are in development.*
- 3.7 *Policies and procedures for requesting physical access to the data center and other MSHP facilities are being updated and modified by the MSHP ISU.*
- 3.8 *A number of administrative and technical controls have either been implemented or are actively being researched by the MSHP to further protect electronic media in transport.*
- 3.9 *Extensive and compliant processes to both sanitize and destroy electronic and physical media are currently employed by the MSHP. The MSHP is working to improve formal documentation of these procedures.*
- 3.10 *The roles and responsibilities for information security have been formally documented and implemented in the information security strategic plan. Job descriptions and classification for ISU personnel are currently being reviewed.*
- 3.11 *Periodic review and re-approval of information security standards, directives and policies are being processed through the information security governance structure. This governance was implemented upon approval of the MSHP's information security strategic plan.*

4. Disaster Recovery Plan

MSHP management has not fully established a disaster recovery plan to ensure the availability of technology resources.

MSHP management has developed certain contingency plans and implemented basic controls for recovery planning. However, the disaster recovery plan has not been (1) fully established, (2) updated to reflect the current processing environment, and (3) fully tested to ascertain the effectiveness of recovery procedures. For example, the plan does not include information that would be necessary should a disaster occur, such as locations of backup data or replacement equipment, responsibilities of key personnel, and procedures to re-establish communications. In addition, since the plan has not been fully developed, a comprehensive test to ensure critical systems can be fully restored has not been performed. A MSHP official said some documented recovery procedures have been implemented but acknowledged the plan is not complete and has not been updated to reflect changes in the operating environment. Certain recovery procedures have also been tested such as recovering data from backups. A MSHP official has been assigned responsibility for creating a new comprehensive disaster recovery plan and staff are currently working on updating the plan.



Criminal Justice Information Security Management Management Advisory Report - State Auditor's Finding

Losing the capability to process and retrieve information can significantly affect an agency's ability to accomplish its mission, according to the GAO. If recovery plans are inadequate, interruptions can result in lost or incorrectly processed data and expensive recovery efforts. Given the implications of mission critical systems not being available for use, it is essential an agency maintains a tested plan to recover critical operations should interruptions occur. According to accepted standards, a disaster recovery plan is a written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities. Recovery plans and procedures are essential steps in ensuring that agencies are adequately prepared to cope with the loss of operational capabilities due to a service disruption such as an act of nature, fire, accident, or sabotage. According to accepted standards, recovery plans should cover all key functions, including assessing an agency's information technology and identifying resources, minimizing potential damage and interruption, developing and documenting the plan, training personnel in their contingency roles and responsibilities and providing refresher training, and testing them and making necessary adjustments.

Without an operational disaster recovery plan, management does not have assurance that technology resources could be restored in the event of a significant disruption to normal system operations and management has limited assurance that data and systems could be recovered and made available to meet requirements in the event of failure at the primary processing location.

Recommendation

The MSHP establish, maintain, and test a comprehensive disaster recovery plan that reflects the current processing environment.

Auditee's Response

The MSHP agrees the existing disaster recovery plan requires updating. The ISU is currently working with the MSHP ICTD to update all aspects of the plan to ensure it is comprehensive and provides adequate protection to all assets. The update, periodic review and testing will be coordinated through the information security governance structure established through the information security strategic plan.

5. National Data Exchange

MSHP management needs to improve controls and procedures to ensure agencies utilizing the National Data Exchange (N-DEx) are in compliance with information security standards, laws, regulations, and requirements for protecting the generation, transmission, use, and storage of CJI.

The Missouri Department of Public Safety established the Missouri Data Exchange System (MoDEX) system, a statewide data warehouse, to provide services to Missouri law enforcement agencies. In 2010, the MoDEX system began interfacing with the N-DEx system, a nationwide data sharing



Criminal Justice Information Security Management Management Advisory Report - State Auditor's Finding

investigative tool administered by the FBI that provides law enforcement agencies with the ability to search, link, analyze and share CJI. According to a MSHP official, during 2013 the MoDEX governing board voted to end support of the MoDEX front end application, which prompted the MSHP to begin utilizing the N-DEx system to allow end user access to this information.

5.1 Audits

MSHP management has not performed audits of agencies with direct access to the N-DEx system. A MSHP official said while these audits are planned to begin in calendar year 2015, agency audits have not been performed since federal auditors will not be auditing the MSHP administration of N-DEx until calendar year 2018.

The CJIS Security Policy requires performing audits at least every 3 years of all agencies with direct access to the system, or that operates workstations, access devices, mobile data terminals, or personal/laptop computers, to ensure compliance with applicable statutes, regulations, and policies. Without conducting audits of agencies, management is unable to effectively ensure agencies are in compliance with applicable statutes, regulations, and policies. In addition, MSHP management faces an increased risk that security weaknesses or control deficiencies are not detected that could compromise the confidentiality, integrity, and availability of CJI maintained by the N-DEx.

5.2 Security awareness training

MSHP management has not established procedures to ensure N-DEx users receive biennial security awareness training. A MSHP official said recertification training is planned to be provided to N-DEx users at some point.

Security awareness includes notifying users of the importance of the information they handle, distributing documentation describing security policies and expected behavior, and requiring users to periodically sign a statement acknowledging their awareness and acceptance of responsibility of security, according to the GAO. Providing training to agency personnel is critical to securing information and information systems since people are one of the weakest links in attempts to secure systems and networks. The CJIS Security and NCIC policies require personnel with physical and logical access to CJI to attend security awareness training within 6 months of initial assignment and biennially thereafter. Dissemination and enforcement of policies are critical as employees cannot be expected to follow policies for which they are not informed, according to accepted standards. Without adequate training, users may not understand system security risks and their role in implementing related policies and controls to mitigate those risks, according to the GAO.



Criminal Justice Information Security Management
Management Advisory Report - State Auditor's Finding

Recommendations

The MSHP:

- 5.1 Perform audits of agencies with access to the N-DEx.
- 5.2 Establish procedures to ensure users with access to the N-DEx are trained and made aware of security responsibilities.

Auditee's Response

- 5.1 *As of April 1, 2015, the MSHP has conducted compliance audits of all Missouri law enforcement agencies accessing N-DEx. These audits cover all areas listed in Section 2.3.2 of the FBI CJIS N-DEx Policy & Operating Manual. The N-DEx component will now be integrated into the MSHP's existing triennial on-site CJIS Systems Audit of all criminal justice agencies. This integration will result in all N-DEx accessing agencies being audited up to two times prior to the FBI's first official N-DEx audit of Missouri in 2018.*
- 5.2 *The ISU is currently working with the CJIS training unit to improve security awareness training delivery to N-DEx users.*