Office of Missouri State Auditor

Nicole Galloway, CPA

Crime Victims' Compensation System Data Security

Report No. 2018-064
August 2018

auditor.mo.gov

Nicole Galloway, CPA
Missouri State Auditor

CITIZENS SUMMARY

Findings in the Audit of Crime Victims' Compensation System Data Security

Data Governance

The Department of Public Safety (DPS) has not established a comprehensive data governance program for the Crime Victims' Compensation (CVC) system. The DPS has not (1) formally established an information technology steering committee to oversee the operations of the CVC system; (2) documented certain existing policies and procedures; (3) fully established a security plan on which department-wide security policies, standards, and procedures can be formulated, implemented, or monitored; (4) completed and documented a formal risk assessment for the CVC system, and (5) established a formal security and privacy awareness training program specifically designed for the CVC system. In addition, the DPS does not have sufficient controls in place to ensure integrity of data and information within the CVC system and to prevent multiple users from editing a single record concurrently.

User Account Management

DPS management has not fully established controls for the creation and maintenance of user accounts for accessing the CVC system. The DPS has not formally documented policies and procedures for requesting, establishing, and maintaining user access to data and other system resources. As of January 2018, one active system account used to convert data from legacy systems into the CVC system remained active when access was no longer required. DPS management has not adequately segregated incompatible functions within the CVC system and has not established controls to limit or detect concurrent access to the CVC system.

System Controls

The DPS does not have adequate controls and procedures to ensure all program activity is properly recorded in the CVC system. The CVC system does not have sufficient logging functionality. The DPS has not established effective controls to ensure system output is compete, accurate, and distributed properly.

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

*****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.

Crime Victims' Compensation System Data Security
Table of Contents

NICOLE GALLOWAY, CPA
Missouri State Auditor

Honorable Michael L. Parson, Governor
and
Charles A. (Drew) Juden, Director
Department of Public Safety
Jefferson City, Missouri

We have audited certain internal controls, including security controls, designed to protect data and information maintained by the Department of Public Safety, Crime Victims' Compensation system. This audit was conducted in fulfillment of our duties under Chapter 29, RSMo. The objectives of our audit were to:

1. Evaluate the system's internal controls over significant management and financial functions.

2. Evaluate compliance with certain legal provisions.

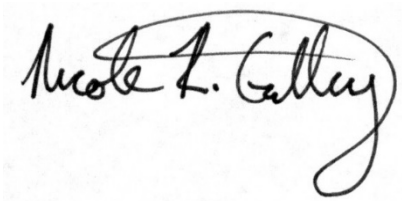
3. Evaluate the economy and efficiency of certain management practices and information system control activities.

4. Evaluate the security and privacy controls designed to ensure the confidentiality, integrity, and availability of data and information maintained in the system.

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 practices and information control activities, and (4) the need to fully establish certain security and privacy controls. The accompanying Management Advisory Report presents our findings arising from our audit of Crime Victims' Compensation System Data Security.

An additional audit of Crime Victims' Compensation System Data Analytics is still in process, and any additional findings and recommendations will be included in that report.



Nicole R. Galloway, CPA
State Auditor

The following auditors participated in the preparation of this report:

Director of Audits:	Jon Halwes, CPA, CGFM
Audit Manager:	Jeffrey Thelen, CPA, CISA
In-Charge Auditor:	Patrick M. Pullins, M.Acct., CISA
Audit Staff:	Kent Aaron Dauderman, M.Acct., CPA

Crime Victims' Compensation System Data Security Introduction

Background

The Missouri Crime Victims' Compensation (CVC) Program is designed to financially assist victims who have sustained bodily or psychological injury in paying for reasonable medical expenses, counseling expenses, funeral expenses, and lost wages or loss of support incurred as a result of being a victim of a crime. The CVC Program is a payor of last resort that pays for financial losses not covered by other sources, such as insurance, worker's compensation, or restitution from the offender.

The CVC Program was established in 1981 under the administration of the Department of Labor and Industrial Relations, Division of Worker's Compensation. By Executive Order 07-07, the program was transferred to the control of the Department of Public Safety (DPS), effective August 28, 2007. The CVC Program is in the DPS Office of the Director.

The current CVC computer system was custom-developed for the state by a third-party contractor and replaced legacy computer systems supporting the program. The department placed the current system into operation in April 2016. Ongoing technical support for the CVC system, including security guidance, the operating environment, and other services is provided by the Office of Administration - Information Technology Services Division (ITSD). In addition to the CVC Program, the computer system also supports the operations of the Sexual Assault Forensic Examination (SAFE) Program and the Child Physical Abuse Forensic Examination (CPAFE) Program.

The Government Accountability Office (GAO) has included the security of information systems, including the protection of Personally Identifiable Information (PII), in the office's High-Risk List since 1997.[1] Technological advances, such as lower data storage costs and increasing interconnectivity, have allowed both government and private sector agencies to collect and process extensive amounts of PII more effectively. Risks to PII can originate from unintentional and intentional threats. These risks include insider threats from careless, disgruntled, or improperly trained employees and contractors; the ease of obtaining and using hacking tools; and the emergence of more destructive attacks and data thefts.

Technology advances, combined with the increasing sophistication of individuals or groups with malicious intent, have increased the risk of PII being compromised and exposed. Correspondingly, the number of reported security incidents involving PII in both the private and public sectors has increased dramatically in recent years. At the same time, state agencies are increasingly reliant on technology and information sharing to interact with

[1] Report GAO-17-317 *Report to Congressional Committees, High Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others,* February 2017, is available at <http://www.gao.gov/assets/690/682765.pdf>.

citizens and to deliver essential services. As a result, the need to protect information, including PII, against cybersecurity attacks is increasingly important.

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. Effective privacy controls depend on the safeguards employed within the information system that is processing, storing, and transmitting PII and the environment in which the system operates. Organizations cannot have effective privacy without a basic foundation of information security. Without proper safeguards and controls, information systems and confidential data are vulnerable to individuals with malicious intentions who can use access to obtain sensitive data or disrupt operations.

The National Institute of Standards and Technology (NIST) defines cybersecurity as the process of protecting information by preventing, detecting, and responding to attacks[2] while ISACA[3] states cybersecurity encompasses all that protects enterprises and individuals from intentional attacks, breaches, and incidents as well as the consequences.[4] Cybersecurity should be aligned with all other aspects of information security, including governance, management, and assurance. The state of being secure requires maintenance and continuous improvement to meet the needs of stakeholders and the demands of emerging cyber threats.

Program funding

The CVC system processes claims for program expenditures from the following funds:

- The Crime Victims' Compensation Federal Fund was established to account for federal monies maintained in the state treasury for the use of the CVC Program. These funds may be received in advance, when related expenditures are made, or after related expenditures are made. Appropriations from this fund authorize disbursements for crime victims' payments.

[2] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, April 2018, is available at <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf >, page 45.
[3] Previously known as the Information Systems Audit and Control Association.
[4] ISACA, *Transforming Cybersecurity: Using COBIT 5*, 2013, page 11.

- The Crime Victims' Compensation Fund was established to award compensation to, or on behalf of, victims of crimes. Appropriations from this fund authorize payments directly to the provider of services for medical or funeral expenses, or expenses for other services as allowed as a payor of last resort for the victim. Other appropriations from this fund pay expenses of the SAFE Program, the statewide crime victim notification system, court automation, and the Office for Victims of Crime. These appropriations are not part of the CVC Program.
- The General Revenue Fund is used for expenditures of the CPAFE Program and other expenditures of the SAFE Program.

Victims may file a claim for payment from the CVC Program for up to 2 years after the date of the crime. The CVC Program reimburses a maximum of $25,000 per claim for crime-related expenses. Some benefit categories have lower limits, which are also included in the $25,000 maximum payout,[5] as follows:

- $400 per week for lost wages
- $5,000 for funeral expenses
- $2,500 for counseling expenses
- $250 for personal property (such as clothing or bedding) seized by law enforcement as evidence of the crime
- Attorney's fees, up to 15 percent of the total award

The primary funding source for the CVC Program is a surcharge of $7.50 assessed as costs on all criminal cases. For all courts, except municipal courts, the fee is collected and the entire amount is remitted to the Department of Revenue (DOR). The first $250,000 collected each fiscal year is deposited to the State Forensic Laboratory Fund. Next, funds are allocated for payments associated with the administrative and operational costs of the Office for Victims of Crime and for the operation of the statewide automated crime victim notification system. Remaining funds are deposited equally to the Crime Victims' Compensation Fund and the Services to Victims Fund. Only the funds deposited to the Crime Victims' Compensation Fund are available to pay the expenses of the CVC Program. Receipts deposited to other funds are used for the purposes of the respective funds.

For surcharges assessed against municipal court cases, the municipality is allowed to retain 5 percent of the collections. The remaining 95 percent of collections is remitted to the DOR, where it is deposited equally between the Crime Victims' Compensation Fund and the Services to Victims Fund.[6]

[5] Sections 595.025 and 595.030, RSMo.

[6] Section 595.045, RSMo.

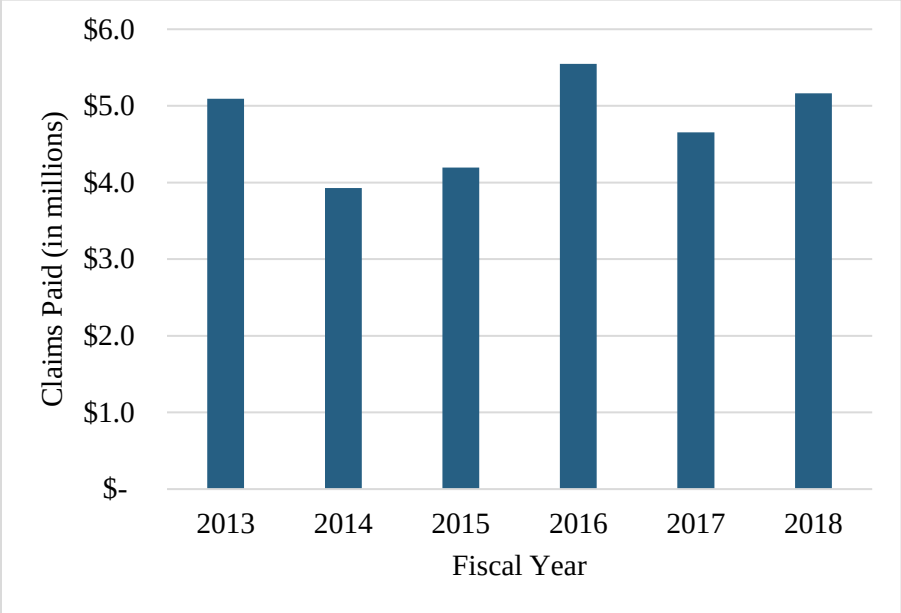
In addition, except in cases of certain specified crimes, each case in which a plea of guilty or a finding of guilt is made, a judgement must be entered against the defendant in the amount of $68 (for a class A or B felony), $46 (for a class C or D felony), or $10 (for a misdemeanor), to be deposited into the Crime Victims' Compensation Fund.

The Crime Victims' Compensation Fund is also allowed to retain interest earnings on the monies in the fund and to receive gifts and contributions for the benefit of victims.

Program payments

Total claims processed through the CVC computer system from the Crime Victims' Compensation Federal Fund and the Crime Victims' Compensation Fund related to the CVC Program during state fiscal years 2013 through 2018 are presented in Figure 1.

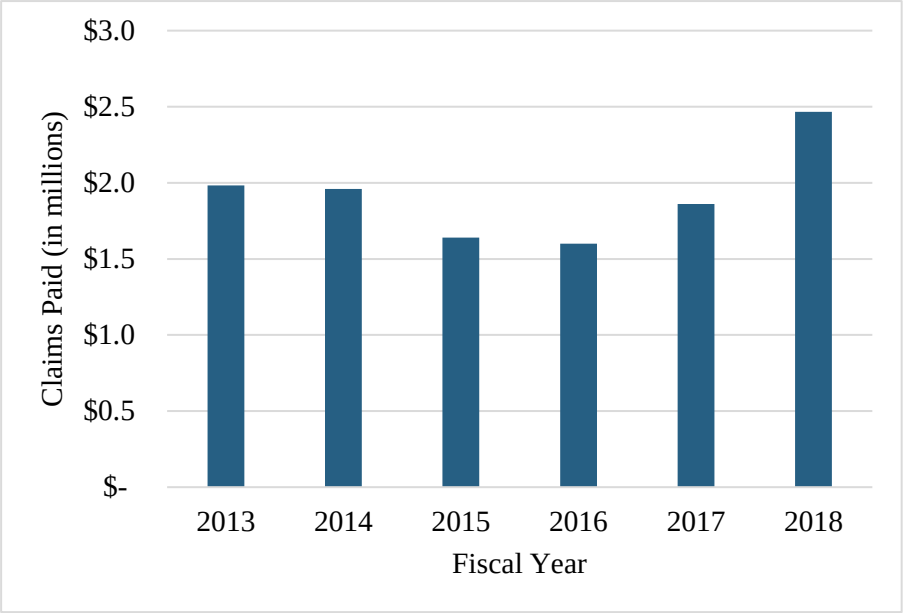
Figure 1: CVC Claims Paid by Fiscal Year



Source: Data from the state's accounting system (SAM II).

Total claims processed through the CVC computer system from the Crime Victims' Compensation Federal Fund and the General Revenue Fund related to the SAFE Program during state fiscal years 2013 through 2018 are presented in Figure 2.

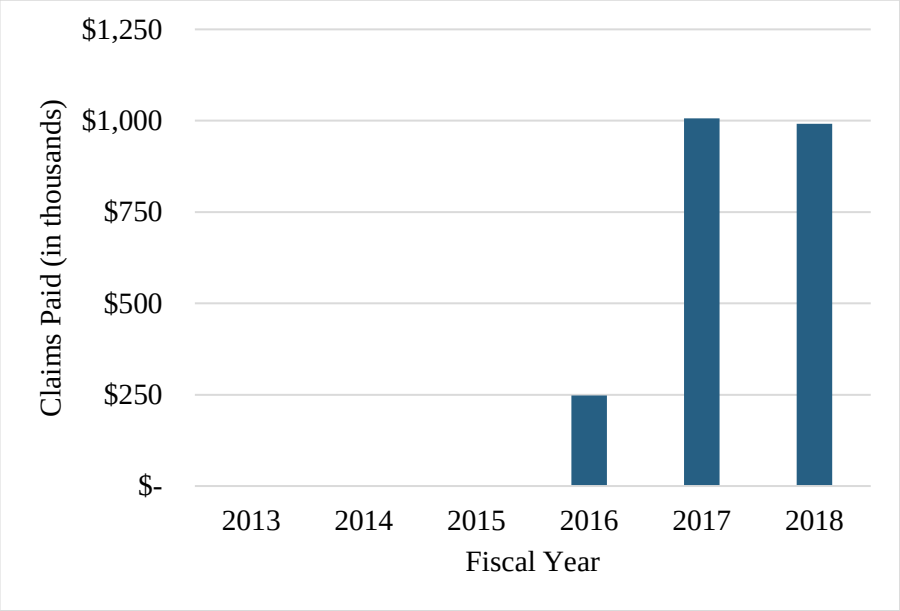
Figure 2: SAFE Claims Paid by Fiscal Year



Source: Data from the state's accounting system (SAM II).

Total claims processed through the CVC computer system from the General Revenue Fund related to the CPAFE Program during state fiscal years 2013 through 2018 are presented in Figure 3. The CPAFE Program was created in fiscal year 2015, with the first expenditures occurring in fiscal year 2016.

Figure 3: CPAFE Expenditures by Fiscal Year



Source: Data from the state's accounting system (SAM II).

Scope and Methodology

The scope of our audit included DPS management's approach to and management of the CVC system, including information security, privacy, and other relevant internal controls; policies and procedures; and other management functions and compliance issues in place during the period April 2016 (when the system was implemented) to June 2018.

Our methodology included reviewing written policies and procedures, and interviewing various DPS personnel. We obtained an understanding of the data governance approach and applicable controls that are significant within the context of the audit objectives and assessed whether such controls have been properly designed and placed in operation. We tested certain of those controls to obtain evidence regarding the effectiveness of their design and operation. We also obtained an understanding of legal provisions that are significant within the context of the audit objectives, and we assessed the risk that illegal acts, including fraud, and violation of contract or other legal provisions could occur. Based on that risk assessment, we designed and performed procedures to provide reasonable assurance of detecting instances of noncompliance significant to those provisions.

We obtained the employment records of all state employees for fiscal years 2001 to 2018 from the statewide accounting system for human resources. We matched these records to the CVC user account records to determine if any terminated employees had active accounts. We identified no terminated state employees with active accounts. Although we used computer-processed data from the human resources 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 of the issues specific to the audit objectives.

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

- Office of Administration - Information Technology Services Division (ITSD)
- National Institute of Standards and Technology (NIST)
- U. S. Government Accountability Office (GAO)
- ISACA (previously known as the Information Systems Audit and Control Association)

Crime Victims' Compensation System Data Security Management Advisory Report
State Auditor's Findings

1. Data Governance

The Department of Public Safety (DPS) has not established a comprehensive data governance program for the Crime Victims' Compensation (CVC) system. As a result, there is less assurance the data management and protection procedures in place are effective in reducing data privacy and security risks due to unauthorized access or misuse of data.

Data governance is defined as an organizational approach to data and information management that is formalized as a set of policies and procedures encompassing the full life cycle of data, from acquisition to use to disposal. It includes establishing policies, procedures, and standards regarding data security and privacy protection, data inventories, content and records management, data quality control, data access, data security and risk management, and data sharing and dissemination, as well as ongoing compliance monitoring of all the above-mentioned activities. By clearly establishing policies, standard procedures, responsibilities, and controls for data activities, a data governance program helps ensure the confidentiality, integrity, and availability of the CVC system.

The responsibility for data governance is shared between the DPS, the system owner; and the Office of Administration - Information Technology Services Division (ITSD), who provides technical support. As system owner, the DPS is responsible for ensuring the system is operating in a secure manner.

1.1 Steering committee

The DPS has not formally established an information technology (IT) steering committee to oversee the operations of the CVC system.

According to the National Institute of Standards and Technology (NIST), it is imperative that leaders and managers at all levels understand their responsibilities and are held accountable for managing information security risk—that is, the risk associated with the operation and use of information systems that support the missions and business functions of their organizations.

In order to carry out this objective, entities should establish an IT steering committee composed of executive, business, and IT management to determine prioritization of IT related projects in line with the enterprise's business strategy and priorities; track status of projects and resolve resource conflicts; and monitor service levels and service improvements, according to accepted standards.

An IT steering committee would take on responsibility for many of the additional tasks discussed throughout this finding. According to management, the DPS has relied on an informal group of CVC system users to fulfill limited steering committee responsibilities.

Without an effective IT steering committee, there is decreased assurance DPS management is effectively designing, implementing, and monitoring controls over the CVC system.

1.2 Policies and procedures

The DPS has not documented certain existing policies and procedures, including those to:

- Formalize ownership of and responsibility for the CVC system.
- Ensure claims are input and processed by the CVC system completely and correctly, including corrections to data as necessary, and that system output accurately reflects such processing.
- Formally establish frameworks necessary to guide and support system security, such as data definitions and classifications, control architecture, periodic reviews of controls, and monitoring procedures.
- Describe procedures to grant, monitor, and remove user accounts, including system, super-user, and emergency accounts.
- Ensure department personnel are aware of expectations and system requirements and that personnel are adequately trained and supervised.

We confirmed the existence of these informal policies and procedures through discussions held with DPS management, who indicated they did not realize the need to formalize these items.

According to accepted standards, documentation of all aspects of computer support and operations is important to ensure continuity and consistency. Formalizing operational practices and procedures with sufficient detail helps to eliminate security lapses and oversights, gives new personnel sufficiently detailed instructions, and provides a quality assurance function to help ensure that operations will be performed correctly and efficiently.

Without documented and approved policies and procedures, management may not have assurance that control activities are appropriate and properly applied.

1.3 Security plan

The DPS had not fully established a security plan on which department-wide security policies, standards, and procedures can be formulated, implemented, or monitored.

An entity-wide information security plan is the foundation of a security control structure and a reflection of senior management's commitment to addressing security risks. The security plan should establish a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. Implementing an information security plan is essential to ensuring controls over information and information systems work effectively

on a continuing basis, according to the Government Accountability Office (GAO).

DPS management indicated they were unaware of the need to complete a security plan and thought the ITSD was responsible for this task. While the ITSD has made available the Missouri Adaptive Enterprise Architecture (MAEA) for consolidated agencies to use as guidance when developing a security plan, the MAEA does not constitute an actual plan for agencies to implement.

Specific plan components missing from the informal CVC security plan include:

- The formal designation of a security administrator responsible for the CVC system with adequate independence, expertise, and authority to define and communicate security procedures and rules of behavior.
- Designation of a framework to be used to formulate, implement, and monitor security policies and procedures.
- Procedures to periodically review and update security practices.

Other components that should be included in the security plan include risk assessments (see section 1.4), security training (see section 1.5), user account management (see Management Advisory Report (MAR) finding number 2), and security logging (see MAR finding number 3).

Until DPS management fully implements a security plan and takes steps to fully develop the necessary policies and controls to correct or mitigate information security control weaknesses, the DPS will have limited assurance that sensitive information and systems are adequately protected.

1.4 Risk assessment

The DPS has not completed and documented a formal risk assessment for the CVC system.

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 assess 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. Only after a risk assessment has been performed can an entity take actions to mitigate

the risks identified, including performance of a cost-benefit analysis and development of an action plan to address risks, according to the MAEA.

While DPS personnel have performed informal risk assessment procedures, a comprehensive risk assessment has not been performed. They indicated a comprehensive risk assessment has not been performed for the CVC system because department management was unaware of the need to perform such an assessment. As such, risk assessment procedures that have been completed have been ad-hoc rather than a comprehensive plan to address risks inherent to the system. Consequently, the department has been unable to formally develop a plan to evaluate, prioritize, and remediate risks to an acceptable level.

Since risks and threats change over time, the results of risk assessments should be documented to ensure an appropriate action plan is developed to limit vulnerabilities and to reduce risk to an acceptable level. The risk assessment should also be performed periodically and revised as necessary whenever there is a change in the entity's operations, according to the GAO.

Without a risk assessment program, DPS management does not have assurance appropriate controls are in place to reduce risks of threats and vulnerabilities to an acceptable level.

1.5 Continuing training

The DPS has not established a formal security and privacy awareness training program specifically designed for the CVC system. As organizations implement more powerful information systems and become more reliant on electronic data, proactive security awareness programs become a priority. Uninformed users are a major threat to data security in organizations.

According to accepted standards, the purpose of security awareness, training, and education is to enhance security by (1) raising awareness of the need to protect system resources; (2) developing skills and knowledge so system users can perform their jobs more securely; and (3) building in-depth knowledge as needed to design, implement, or operate security programs for organizations and systems.

Making computer system users aware of their security responsibilities and teaching them correct practices helps users change their behavior. Awareness training also supports individual accountability, which is one of the most important ways to improve information security. With proper security and privacy awareness training and clear communication of data and device use policies, employees can become the first line of defense against cybersecurity incidents. However, without adequate training, users may not understand system security risks and their role in implementing related policies and controls to mitigate those risks.

DPS management indicated employees participate in the ITSD's statewide information security awareness program. However, the ITSD program only covers general security and privacy controls and is not specific to the CVC system. As such, additional training is needed for DPS staff regarding specific security requirements of the CVC system and program.

1.6 Data integrity

The DPS does not have sufficient controls in place to ensure integrity of data and information within the CVC system and to prevent multiple users from editing a single record concurrently.

Data integrity exists when data agrees with its source and has not been accidentally or maliciously modified, altered or destroyed, according to accepted standards. Integrity is lost if unauthorized changes are made to the data or system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccurate data, fraud, or erroneous decisions. DPS staff indicated they monitored data integrity during the conversion from the legacy CVC systems to the current system; however, that control has not continued and procedures to ensure the continued integrity of data have not been established.

In addition, a record-locking control to prevent two users from simultaneously editing the same record in the CVC system is not in place. A record-locking control allows only one user to modify a record at any given time in order to prevent incompatible edits and preserve data integrity. If a record-locking control is not in place, a user is not restricted from making changes to a record while another user is accessing the same record, which increases the risk of inaccurate transaction records as well as any associated reports. According to DPS management, concurrent updating had not been considered until we discussed the issue with them. Establishing a record-locking control requires working in conjunction with the ITSD to develop a system enhancement.

According to accepted standards, data integrity management requires an organization to define and document policies and procedures to ensure integrity and consistency of data. This process improves the quality of management decision-making by helping to ensure reliable and secure information is provided.

Conclusion

Without fully establishing a data governance program in coordination with all responsible entities, management faces an increased risk that security and privacy controls will not be effective or operate as designed, leaving the CVC system more vulnerable to threats and impacting the confidentiality, integrity, and availability of CVC Program data.

Recommendations

The DPS:

1.1 Form an IT steering committee to oversee the management and operation of the CVC system.

1.2 Fully document and periodically review policies and procedures.

1.3 Fully develop and document a formal security plan for the CVC system.

1.4 Design and implement a formal risk assessment process that includes policies, standards, and procedures for performing periodic risk assessments and for reducing risk to an acceptable level.

1.5 Establish a formal security and privacy awareness training program for the CVC system.

1.6 Develop and document formal procedures for monitoring and maintaining the integrity of data stored in the CVC system. In addition, work with the ITSD to establish a record-locking control for preventing concurrent editing.

Auditee's Response

1.1 The DPS has maintained an informal committee regarding management and operations of the CVC computer system since the system launched in 2016. During this audit, the DPS formulated a plan to formalize a steering committee for the CVC system. This plan also creates an Information Technology Systems Analyst (ITSA) position, which the DPS filled in April 2018. The ITSA will lead the creation of written processes and lead quarterly committee meetings. The DPS will establish a formal steering committee by October 1, 2018.

1.2 The DPS has recognized the need to better document its policies and procedures. It began revamping its policies and procedures manual in the spring of 2018, and this process is ongoing. After completion, the document will be reviewed periodically for compliance with changes in regulations and practice. Additionally system specific policies and procedures are scheduled to be developed in conjunction with the security plan.

1.3 The DPS recognizes the value of a formal security plan for the CVC system. The ITSA along with the ITSD, has been directed to create a security plan following completion of the CVC system risk assessment. This plan will designate the ITSA as the security administrator. The security plan will include a periodic review timetable and a framework to monitor security procedures.

1.4 The DPS has maintained informal risk assessment procedures since launching the current CVC computer system in 2016. During this audit, the DPS created a plan to formalize these risk assessment procedures in order to evaluate, prioritize, and remediate risks inherent to the CVC system. As noted above, the DPS hired an ITSA in April 2018, who will lead the creation of written risk assessments and the mitigation of threats.

1.5 The DPS is eager to further educate our staff on general security and privacy controls provided by the ITSD, including security and privacy controls specific to the CVC system. Upon completion of the policy manual revision, the DPS will implement a training program that includes risk assessment security, user account management, PII safeguard, and other appropriate subjects.

1.6 The DPS recognizes the value of formally reviewing data integrity through controls of the CVC system. Your rigorous testing has helped the DPS identify areas for potential improvement. The ITSA, DPS, and ITSD are partnering to improve and limit the risk of modifications to the CVC system. The DPS has requested the ITSD's assistance on improving the CVC system's data integrity, including potentially implementing the suggested record locking capabilities.

2. User Account Management

DPS management has not fully established controls for the creation and maintenance of user accounts for accessing the CVC system. Existing procedures for granting user access to the CVC system need to be strengthened and documented. Accounts used for support purposes were not removed once no longer required, and inactive accounts were allowed to remain in the user listing. In addition, security roles available to users are not restricted to only those functions necessary to do assigned jobs; roles with super-user capabilities were assigned to system support staff; and controls have not been established to restrict users from accessing the system from multiple locations concurrently.

2.1 Account requests

The DPS has not formally documented policies and procedures for requesting, establishing, and maintaining user access to data and other system resources. Additionally, a standard user access request form is not used to document the request and approval process.

User account control activities include requesting, establishing, issuing, suspending, modifying, closing, and periodically reviewing user accounts and related user privileges, according to accepted standards. To adequately control accounts, an organization should establish policies and procedures for authorizing and maintaining all user accounts, including system administrators. These policies and procedures should cover user access needed for routine operations, emergency access, and the sharing and

disposition of data with individuals or groups outside the organization. DPS management indicated they were unsure why such policies and procedures had not been established.

Accepted standards also require access authorizations to be documented on standard forms and approved by resource owners, and listings of authorized users to be maintained. A formal process for transmitting these authorizations should be established to reduce the risk of mishandling, alterations, and misunderstandings.

Without appropriate account access policies and procedures, users may be granted inappropriate or unauthorized access, which can provide opportunities for misuse or inappropriate disclosure of sensitive data.

2.2 User account issues

As of January 2018, one active system account used to convert data from the legacy systems into the CVC system remained active when access was no longer required. We discussed this account with DPS management in April 2018, and the account was disabled in May 2018. DPS management indicated this error went undetected because their review of users focused only on DPS employees, and not system accounts.

As of January 2018, 69 inactive user accounts existed in the CVC system user listing. These accounts are assigned to users who no longer need access to the CVC system as part of their job duties or who had left employment. DPS management indicated these accounts are assigned to inactive status rather than being deleted to preserve the integrity of system logs. However, these accounts could accidentally or maliciously be reactivated, allowing users to regain their access to the CVC system. This weakness is especially critical given that most of these accounts belong to ITSD employees who, although no longer working on the CVC system, are still state employees working on other projects. If one of these user account was reactivated, the user could inappropriately regain access to the CVC system.

After we discussed this issue with DPS management, they created a new role within the system that is not assigned any actual access rights. All inactive user accounts were assigned to this role, meaning that even if the accounts were to be accidentally reactivated, users could not access any information in the system without also changing the role.

Without effective procedures to remove access, terminated employees and system accounts that are no longer required could continue to have access to critical or sensitive resources or have opportunities to sabotage or otherwise impair entity operations or assets, according to the GAO.

2.3 Segregation of duties

DPS management has not adequately segregated incompatible functions within the CVC system.

We found certain access roles allowed users to perform incompatible functions. For example, four different access roles allow user accounts the ability to create, update, and approve claims; approve or deny the payment of a claim; delete a claim; edit reference tables; and modify system reference tables. One of these four roles was assigned to multiple ITSD support personnel, who had complete access to every portion of the CVC system. Additionally, we found two roles with identical access rights to the system, which can cause additional administrative burden. DPS management could not explain why the roles were assigned in this manner.

Inadequately segregated duties increase the risk that erroneous or fraudulent transactions could be processed, that improper program changes could be implemented, and that computer resources could be damaged or destroyed, according to the GAO.

2.4 Concurrent access

The DPS has not established controls to limit or detect concurrent access to the CVC system.

Concurrent session controls prevent a single user from accessing an information system from more than a specified number of locations at any given time. These controls help prevent unauthorized users from accessing the system by masquerading as an authorized user. DPS management was unaware of the need to limit concurrent access.

According to accepted standards, the number of concurrent sessions for a user should be limited. Without limiting or detecting access from multiple locations at the same time, management may not be able to ensure the confidentiality, integrity, and availability of data and the system.

Recommendations

The DPS:

2.1 Fully establish and document formal policies and procedures, including requiring standard forms, for requesting, approving, and maintaining access to the CVC system.

2.2 Periodically review user accounts to ensure access that is no longer necessary is removed timely.

2.3 Perform a comprehensive review of the CVC user access roles to ensure incompatible functions are identified and properly segregated.

2.4 Manage and monitor the number of concurrent sessions for a single user.

Auditee's Response

2.1 The DPS has maintained an informal process for requesting and removing user access in the CVC system. This system required

supervisor approval for changes in user access status, and used ITSD records as documentation of these changes. Following this audit, the DPS will formalize the process as described in this recommendation. The ITSA will lead these changes, which will be included in the DPS's written policies and procedures.

2.2 The DPS concurs in the need for periodic review of user accounts, including a formal process and timetable. The ITSA has been tasked with developing new procedures to ensure that the right level of access is provided to user accounts, including a biannual review of roles access to minimize user privileges.

2.3 The DPS concurs in this recommendation. The ITSA will initiate development of a formal process and timetable to accomplish this recommendation. This will include development of user- and role-based access to CVC systems, and a biannual review of roles access to minimize user privileges. After development, these processes will be included in the DPS's written policies and procedures.

2.4 The DPS recognizes the concerns regarding concurrent access of the CVC system. These concerns are limited as the CVC system is only accessible within the state network with state credentials monitored by ITSD. The ITSA, DPS, and ITSD will meet to discuss limiting the risk of concurrent sessions in the CVC system and the feasibility of implementing this recommendation.

3. System Controls

The DPS does not have adequate controls and procedures to ensure all program activity is properly recorded in the CVC system. The system does not sufficiently log certain events and does not provide appropriate reports or data to account for system output.

3.1 System logs

The CVC system does not have sufficient logging functionality. In addition, the current logging functionality does not record all necessary details for monitoring certain document processing and security-related activities.

The CVC system is accessed via the state's internal computer network. Access to the system is controlled via the ITSD's consolidated network security application. Accordingly, many security events, such as network logon are recorded in the logs maintained by the ITSD and are not subject to logging within the CVC application itself.

The CVC system contains event logging functionality within the claim processing component of the application. However, this log only writes records when documents are uploaded to the application and when the system generates documents to be sent to the claimant. If a user were to delete an uploaded document or modify the underlying claim, that activity is not

logged. Additional items not logged include system-specific security functionality such as changes in what roles a user is assigned to, changes in what system functionality a role grants access to, or modifications to the logs themselves. This enhanced logging functionality is not currently available in the CVC system. DPS management indicated they relied on the ITSD for logging and were not aware of the limited CVC system logging functionality. They agreed the logging functions should be reviewed and improved if they added value.

Without an effective method to identify, log, and monitor significant security-relevant events, management faces an increased risk that unauthorized or inappropriate system activity may not be detected.

3.2 Output controls

The DPS has not established effective controls to ensure system output is compete, accurate, and distributed properly.

When a claim is approved for payment in the CVC system, several steps must be completed to distribute the payment to the claimant. An automated interface sends a check request to the state's accounting system, which causes a check to be printed and returned to the department. The CVC system also generates printed letters to the claimant and produces various electronic reports available to authorized users. This daily activity is summarized into various monthly, quarterly, and annual reports.

The DPS currently relies on manual controls to ensure output is complete and accurate. For instance, staff manually match checks generated by the accounting system to letters generated by the CVC system. However, this procedure would fail to detect instances where both a check and a letter were not created, or where the documents may have been intercepted or tampered with.

DPS management told us they believe the manual controls currently in place are sufficient to control system output. The manual procedures used by DPS staff to reconcile various reports at the end of each month would detect if the reports were out of balance. However this procedure could be enhanced by making it an automated alert that compares data daily, detecting errors or issues more timely.

Without effective output controls, the DPS is at increased risk that inaccurate payments, whether caused by system errors or malfeasance, could occur and not be detected timely.

Recommendations

The DPS:

3.1 Work with the ITSD to determine what application-level security events and incidents should be logged and monitored and develop such functionality.

3.2 Implement more effective controls over CVC system outputs.

Auditee's Response

3.1 The DPS concurs that there is value in reviewing the logging functions to determine if there is an opportunity to add value through change in functionality. Testing has discovered some areas of improvement. The DPS will work with the ITSD to enhance the CVC system's logging capabilities.

3.2 At this time, the manual controls currently in place for the CVC system are sufficient for the needs of the program. Physical checks issued by the state's SAM II payment system are matched with letters prepared by the CVC computer system. These independent systems provide safeguards that guard against waste, fraud, and abuse.