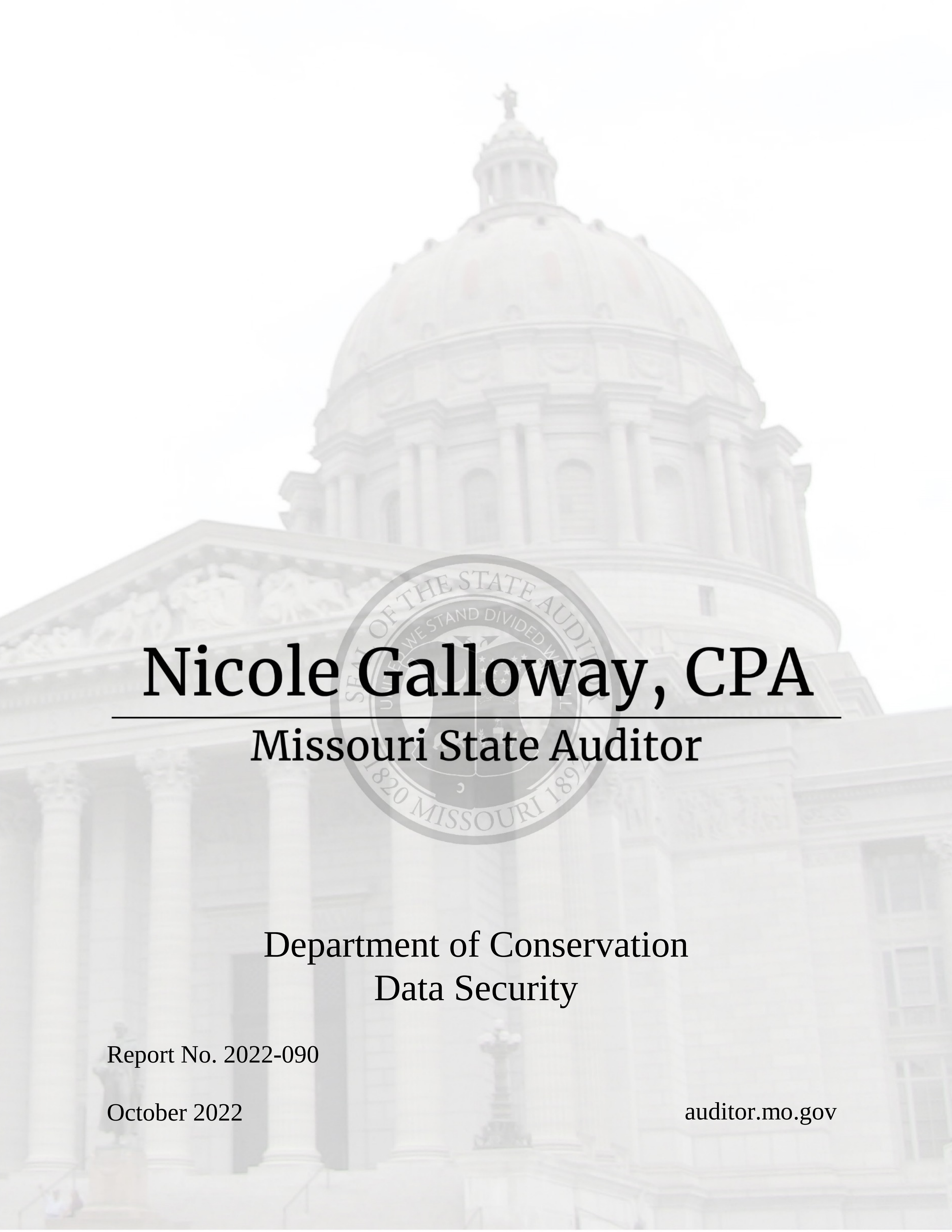


Nicole Galloway, CPA

Missouri State Auditor

Department of Conservation
Data Security

Report No. 2022-090

October 2022

auditor.mo.gov

October 2022

Nicole Galloway, CPA
Missouri State Auditor

CITIZENS SUMMARY

Findings in the audit of the Department of Conservation Data Security

User Account Management	The Missouri Department of Conservation (MDC) does not always timely remove accounts of terminated users and does not ensure a network security system control requiring user accounts' passwords to be changed periodically is consistently enforced. The MDC does not proactively monitor for user accounts that have not been accessed or used for a specified period of time and does not have a policy requiring such review. The MDC does not perform periodic reviews of existing users' access to resources to ensure access remains appropriate and aligned with job responsibilities, nor is there a policy requiring such reviews.
Service Level Agreement	The MDC and the Office of Administration - Information Technology Services Division (ITSD) do not have a service level agreement in place for IT services provided by the ITSD to the MDC.
Policies and Procedures	The MDC has not formally completed and documented a comprehensive risk assessment program. The MDC has not fully established a security plan on which department-wide security policies, standards, and procedures can be formulated, implemented, or monitored. The MDC has not documented policies and procedures for certain security controls of department systems.

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.

Department of Conservation Data Security
Table of Contents

State Auditor's Report 2

Introduction

Background 3
Scope and Methodology 5

Management Advisory Report - State Auditor's Findings

1. User Account Management 6
2. Service Level Agreement 9
3. Policies and Procedures 10

Appendix

Department of Conservation Response 14

NICOLE GALLOWAY, CPA
Missouri State Auditor

Honorable Michael L. Parson, Governor
and
Sara Parker Pauley, Director
Missouri Department of Conservation
Jefferson City, Missouri

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

1. Evaluate the department's internal controls over significant management operations, including the effectiveness of information security controls and other management practices for protecting the confidentiality, integrity, and availability of significant systems and information.

2. Evaluate the department's compliance with certain legal provisions.

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, and (2) no significant noncompliance with legal provisions.

The accompanying Management Advisory Report presents our findings arising from our audit of Missouri Department of Conservation Data Security.

Nicole R. Galloway

Nicole R. Galloway, CPA
State Auditor

Background

The mission of the Missouri Department of Conservation (MDC) is to protect and manage the fish, forest, and wildlife resources of the state; and to facilitate and provide opportunity for all citizens to use, enjoy, and learn about these resources. The MDC Information Technology (IT) Branch supports the department's mission through technological solutions and electronic communications. The MDC was not included in the 2005 statewide consolidation of IT resources, but works closely with the consolidated IT operations on certain matters.

The IT Branch provides support and management of information technology resources for the MDC. Information, some of which is sensitive, maintained in MDC systems includes:

- Hunting and fishing permits and licenses
- Wildlife protection investigations and arrests
- Human resource and department expenditure records
- Geographic information system data

To carry out its duties, the MDC uses approximately 125 various applications to collect, process, and distribute information. These applications are a combination of those developed and supported by internal MDC personnel, as well as those developed by contractors. These applications support functions including administration, permitting and licensing, investigations, environmental protection, mapping, and natural resource protection, among other functions.

Disclosure of specific sensitive data maintained in MDC systems could compromise department enforcement activities. In addition, unauthorized access to personal information could increase the risk of identity theft.

The Government Accountability Office (GAO) has included the security of information systems in the office's High-Risk List since 1997, specifically adding the protection of Personally Identifiable Information (PII) in its 2015 update.[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.

[1] GAO, Report GAO-21-119SP *Report to Congressional Committees, High Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, March 2021, p.168, <https://www.gao.gov/assets/gao-21-119sp.pdf>, accessed June 17, 2022.

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

According to the National Institute of Standards and Technology (NIST),[2] security controls are the safeguards or countermeasures employed within a system or an organization to protect the confidentiality, integrity, and availability of the system and its information and to manage information security risk. 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 NIST defines cybersecurity as the process of protecting information by preventing, detecting, and responding to attacks[3] while ISACA 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.

[2] NIST, Special Publication 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, p. 1, 396, 398, and 406, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>, accessed June 17, 2022.

[3] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, April 2018, p. 45, <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>, accessed June 17, 2022.

[4] ISACA, *Transforming Cybersecurity*, 2013, p. 11.

Scope and Methodology

The scope of our audit included evaluating (1) MDC management's approach to and management of information security controls; (2) policies and procedures; and (3) other management functions and compliance issues in place during the year ended December 31, 2021.

Our methodology included reviewing written policies and procedures, interviewing various MDC personnel, and performing testing. We obtained an understanding of internal control that is significant to the audit objectives and planned and performed audit procedures to assess internal control to the extent necessary to address the audit objectives. 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 reviewed the authorized users for the MDC network, as well as a separate contractor-developed system, to determine if any terminated employees had active user accounts. In addition, we obtained employment records of all state employees from the statewide accounting system, Statewide Advantage for Missouri (SAM II), and matched these records against all authorized users. We provided MDC management a list of all terminated employees identified. Although we used computer-processed data from the MDC network, contractor system, and SAM II for our audit work, we did not rely on the results of any processes performed by these systems in arriving at our conclusions. Our conclusions were based on our review of the issues specific to the audit objectives.

We also assessed user access to PII maintained by the MDC.

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

- Missouri Adaptive Enterprise Architecture (MAEA)
- National Institute of Standards and Technology (NIST)
- Government Accountability Office (GAO)
- ISACA

1. User Account Management

The Missouri Department of Conservation (MDC) does not always timely remove accounts of terminated users, and has not consistently or adequately established certain user account controls. As a result, information maintained by the MDC is at risk of inappropriate access.

The MDC uses various internally-developed and contractor-developed information systems to carry out its functions. In addition, the MDC purchases or licenses various commercially available software products. User access to these systems is either controlled by a network security system maintained by the MDC or through a security system specific to an individual system. The MDC network security system is designed to allow users access from both onsite and remote locations.

A contributing factor to the account management weaknesses identified is a lack of comprehensive policies and procedures for the management of user accounts. Additional concerns regarding departmental policies and procedures are discussed in Management Advisory Report (MAR) finding number 3.

1.1 Terminated and unidentified users

Accounts of terminated users are not always removed timely, which leaves the MDC vulnerable to the risk of records being improperly viewed and altered. A terminated user is someone who has left employment with an entity and no longer needs access to the entity's data. We tested all MDC user accounts and found concerns with 39 users' access to the MDC network. Of those 39 user accounts identified, 31 users were former employees whose employment had ended at least 30 days prior to our test, and MDC could not identify the remaining 8 users, or determine why their access to MDC resources was necessary. In addition, we identified 8 terminated users with access to MDC resources via a separate, contractor-developed system. One of these users terminated employment in February 2019, 5 in 2021, and the termination dates for 2 were unknown.

While the MDC has a documented policy describing user termination procedures, department information technology (IT) management indicated IT staff turnover contributed to the failure to detect and remove terminated users timely. Additionally, MDC policy does not address accounts in the contractor-developed system.

According to the Missouri Adaptive Enterprise Architecture (MAEA),[5] entities must have a procedure in place for the timely notification of

[5] The MAEA includes standards, policies, and guidelines established by Office of Administration management. The MAEA is made up of several information technology domains, including domains dedicated to security and information. The domains define the principles needed to help ensure the appropriate level of protection for the state's information and technology assets.

administrators when a user no longer needs access. In addition, entities are responsible for determining who is given access to their systems and for ensuring all individuals who have access still need the access. When a user no longer needs access, the entity should submit a form to the security administrator requesting removal of the user's access to the systems.

Without effective procedures to remove access, terminated employees 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 Government Accountability Office (GAO).[6]

1.2 Password expiration

The MDC does not ensure a network security system control requiring user accounts' passwords to be changed periodically is consistently enforced. IT management verbally indicated their practice is to consistently enforce this control; however, the department does not have a formal written policy requiring it. We found 44 user accounts whose passwords were set to never expire.

Password controls reduce the risk of unauthorized access to computers and data. The MDC requires passwords to authenticate network access, and established a policy requiring passwords to be changed periodically. The network security system allows administrators to specify the maximum length of time that a password may be used. After this maximum time, a user is required to change the password. This policy is consistent with MAEA requirements that passwords for all systems be subject to password expiration. However, the MDC does not consistently enforce this control for all users.

Allowing accounts to have non-expiring passwords greatly increases the risk of an account password becoming known by someone other than the account owner, which may result in inappropriate access to and misuse of sensitive department information.

1.3 Inactive user accounts

The MDC does not proactively monitor for user accounts that have not been accessed or used for a specified period of time and does not have a policy requiring such review. Department IT management indicated this review did not happen due IT staff turnover.

Our analysis of system user accounts identified 14 accounts that had never been accessed by the user assigned to the account. This may indicate the access was not necessary and should not have been granted. We also identified 70 accounts that had not been accessed for an extended period.

[6] GAO, Report GAO-09-232G, *Federal Information System Controls Audit Manual*, February 2009, p. 176 and 225, <https://www.gao.gov/assets/gao-09-232g.pdf>, accessed June 17, 2022.

NIST guidance recommends system administrators disable inactive accounts after a specified time period.[7] This reduces opportunities for inappropriate system access, potentially by individuals who do not own the account. Without appropriate monitoring, security administrators are less likely to identify user accounts that have not been accessed or used for a specified period of time.

1.4 Existing user access

The MDC does not perform periodic reviews of existing users' access to resources to ensure access remains appropriate and aligned with job responsibilities, nor is there a policy requiring such reviews.

As users' job responsibilities change, access rights to resources may be added, changed, or removed. Over time, users can accumulate access rights that are no longer necessary, increasing the risk of inappropriate access.

Without periodically reviewing user access rights, there is an increased risk that unauthorized alterations of the rights will go undetected or that access rights may not be aligned with current job responsibilities.

Recommendations

The MDC:

1.1 Ensure user access is adequately reviewed to identify and remove accounts belonging to terminated employees and unidentified users in accordance with policy. In addition, the policy should be updated to cover the contractor-developed system.

1.2 Develop a policy to ensure user account passwords are consistently set to periodically expire.

1.3 Develop a policy to periodically monitor for user accounts that have not been accessed or used for a specified period of time.

1.4 Develop a policy to ensure existing users' access rights are periodically reviewed and remain appropriate and aligned with job responsibilities.

Auditee's Response

The department's written response is included in the Appendix.

[7] NIST, Special Publication 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations,* p. 20-21, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>, accessed June 17, 2022.

2. Service Level Agreement

The MDC and the Office of Administration (OA) - Information Technology Services Division (ITSD) do not have a service level agreement (SLA) in place for IT services provided by the ITSD to the MDC. As a result, the responsibilities and expectations between both parties are not fully established or documented.

The MDC did not participate in the 2005 consolidation of IT services from most other state agencies into the centralized ITSD. Therefore, the MDC is solely responsible for IT services necessary for its business operations. However, the MDC works with the ITSD to obtain certain services. Services provided by the ITSD include state network access, security monitoring, and access to statewide IT contracts, among others.

An SLA is a document used by organizations entering into a partnership for the provision of IT services. According to ISACA, an SLA is used to align IT enabled products and services and service levels with enterprise needs and expectations, including identification, specification, design, publishing, agreement, and monitoring of IT products and services.[8] SLAs can be in-house between an organizational unit and its IT department, external between an entity and an outside service provider, or internal within the units of a service provider.[9]

MDC management indicated they were not aware of the need for an SLA, and that operations between the ITSD and MDC had been operating well without one. However, an SLA is crucial to promote continuous and open communication between the parties to the agreement. Without such communication, there is an increased risk the customer and the service provider will not appropriately understand or respond to each other's expectations. This weakness could result in confusion or frustration, or potentially more severe outcomes such as system failure or data loss.

According to the *Information Systems Control Journal*,[10] an "SLA is a necessity between a service provider and service beneficiary because a service can be called 'bad' or 'good' only if this service is clearly described. Moreover, it formalizes the needs and expectations of the organization and serves as a kind of guarantee for both parties. In this way, potential misunderstandings are reduced and a clear view is given on the priorities of the service and its delivery. . . . A balanced SLA is a compromise between the needs, expectations and requirements of the organization (user group) and

[8] ISACA, *Control Objectives for Information and Related Technologies 2019 Framework: Governance and Management Objectives*, November 2018, p. 113-115.
[9] Van Grembergen, Wim, Ph.D., Steven De Haes and Isabelle Amelinckx. "Using COBIT and the Balanced Scorecard as Instruments for Service Level Management." *Information Systems Control Journal*, Volume 4 (2003): p. 56.
[10] Ibid., p. 56-57.

the service provision capabilities and promises of the service provider. At the same time, it must protect the service provider by limiting liability, identifying responsibilities and rationally managing user expectations."

Recommendation

The MDC work with the ITSD to develop an SLA that specifies services to be provided and addresses communications between the agencies.

Auditee's Response

The department's written response is included in the Appendix.

3. Policies and Procedures

MDC management has not developed certain key policies and procedures for data security. Additionally, some polices that have been developed have not been formally documented.

3.1 Risk assessment

The MDC has not formally completed and documented a comprehensive risk assessment program.

According to the National Institute of Standards and Technology (NIST),[11] risk assessments are used to identify, estimate, and prioritize risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and other organizations, resulting from the operation and use of information systems. Risk is determined by identifying potential threats, identifying vulnerabilities in systems, determining 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. 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. According to the MAEA, 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.

While MDC personnel have performed informal risk assessment procedures, a comprehensive risk assessment has not been performed. 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.

Since risks and threats change over time, the results of risk assessments should be documented to ensure an appropriate action plan is developed to

[11] NIST, Special Publication 800-30 Revision 1, *Guide for Conducting Risk Assessments*, September 2012, <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>, accessed June 17, 2022.

limit vulnerabilities and to reduce risk to an acceptable level. According to the GAO,[12] the risk assessment should also be performed periodically and revised as necessary whenever there is a change in the entity's operations.

Without a comprehensive risk assessment program, MDC management has less assurance appropriate controls are in place to reduce risks of threats and vulnerabilities to an acceptable level.

3.2 Security plan

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

According to the GAO,[13] 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.

MDC management indicated the department has informally adopted the Center for Internet Security's (CIS) Critical Security Controls framework to guide cyber security operations. The MDC has also partially completed a self-evaluation based on the CIS controls to identify security risks to address. However, the use of this framework has not been formally approved, nor has a complete evaluation been performed.

Until MDC 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 MDC will have limited assurance that sensitive information and systems are adequately protected.

3.3 Documentation of security controls

The MDC has not documented policies and procedures for certain security controls of department systems.

According to the GAO,[14] control activities are the policies, procedures, techniques, and mechanisms that enforce management's directives and help

[12] GAO, Report GAO-09-232G, *Federal Information System Controls Audit Manual*, February 2009, p. 167-169, <https://www.gao.gov/assets/gao-09-232g.pdf>, accessed June 17, 2022.

[13] Ibid, p. 151.

[14] GAO, Report 14-704G, *Standards for Internal Control in the Federal Government*, September 2014, p. 75, <https://www.gao.gov/assets/gao-14-704g.pdf>, accessed June 17, 2022.

ensure that actions are taken to reasonably address risks. The following control activities have not been fully documented:

- Incident response, reporting, and correction
- Continuity planning and disaster recovery procedures, including system and data backups and recovery procedures
- Data and resource ownership, and owner responsibilities
- Security logging and monitoring
- Physical security procedures, including visitor access
- Segregation of duties
- Security training and awareness
- Password standards and requirements
- Privileged user account access

MDC staff indicated that much of this information is communicated to users by on-the-job training and other informal processes.

According to NIST,[15] 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 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.

Recommendations

The MDC:

3.1 Design and implement a formal risk assessment process that includes policies, standards, and procedures for performing periodic risk

[15] NIST, Special Publication 800-12 Revision 1, *An Introduction to Information Security*, June 2017, p. 49, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf>, accessed June 17, 2022

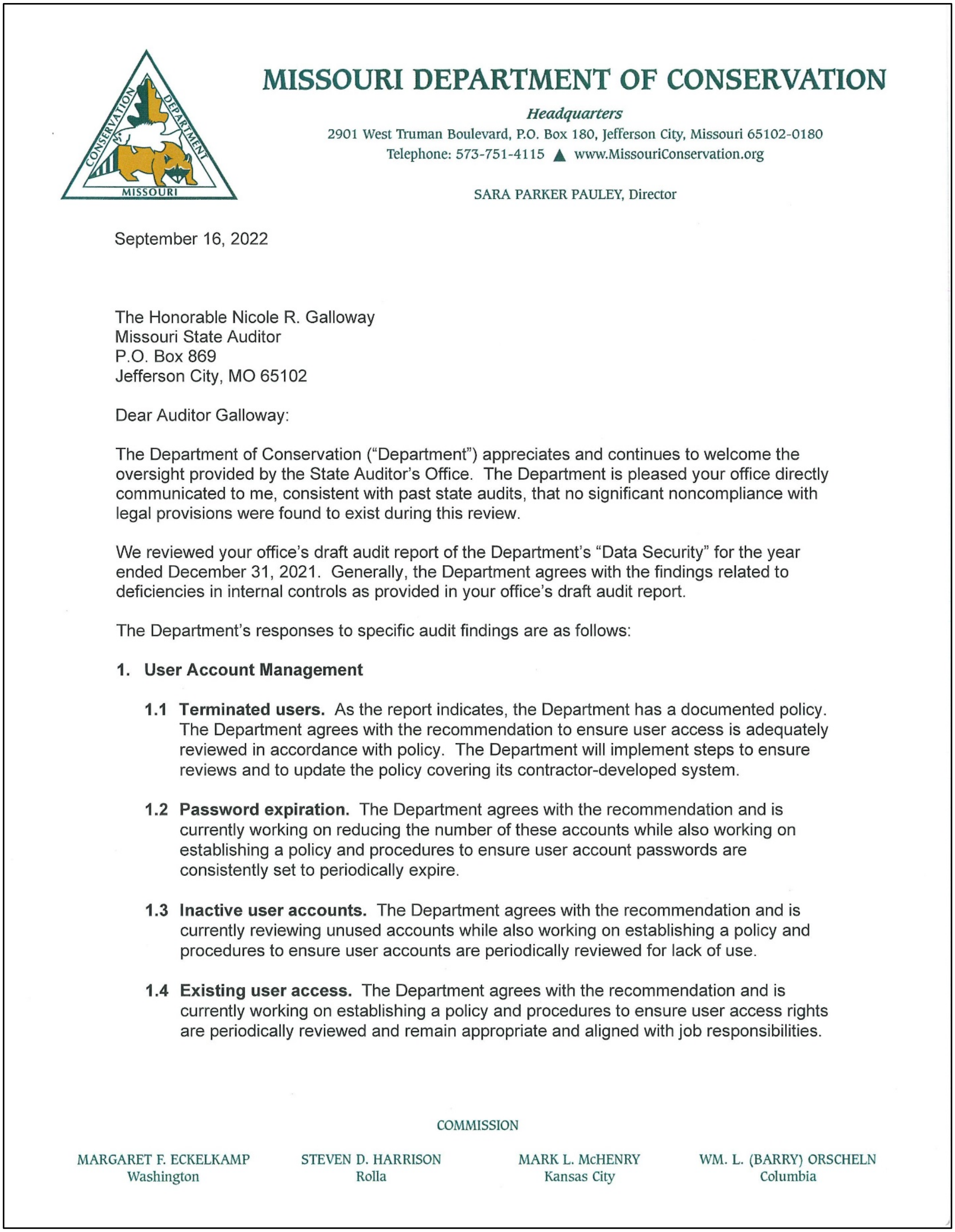
assessments and for reducing risk to a level acceptable to the department.

3.2 Fully develop and document a formal security plan for MDC systems.

3.3 Fully document and regularly review documentation of key security controls.

Auditee's Response

The department's written response is included in the Appendix.



MISSOURI DEPARTMENT OF CONSERVATION

Headquarters
2901 West Truman Boulevard, P.O. Box 180, Jefferson City, Missouri 65102-0180
Telephone: 573-751-4115 ▲ www.MissouriConservation.org

SARA PARKER PAULEY, Director

September 16, 2022

The Honorable Nicole R. Galloway
Missouri State Auditor
P.O. Box 869
Jefferson City, MO 65102

Dear Auditor Galloway:

The Department of Conservation ("Department") appreciates and continues to welcome the oversight provided by the State Auditor's Office. The Department is pleased your office directly communicated to me, consistent with past state audits, that no significant noncompliance with legal provisions were found to exist during this review.

We reviewed your office's draft audit report of the Department's "Data Security" for the year ended December 31, 2021. Generally, the Department agrees with the findings related to deficiencies in internal controls as provided in your office's draft audit report.

The Department's responses to specific audit findings are as follows:

1. **User Account Management**

   1.1 **Terminated users.** As the report indicates, the Department has a documented policy. The Department agrees with the recommendation to ensure user access is adequately reviewed in accordance with policy. The Department will implement steps to ensure reviews and to update the policy covering its contractor-developed system.

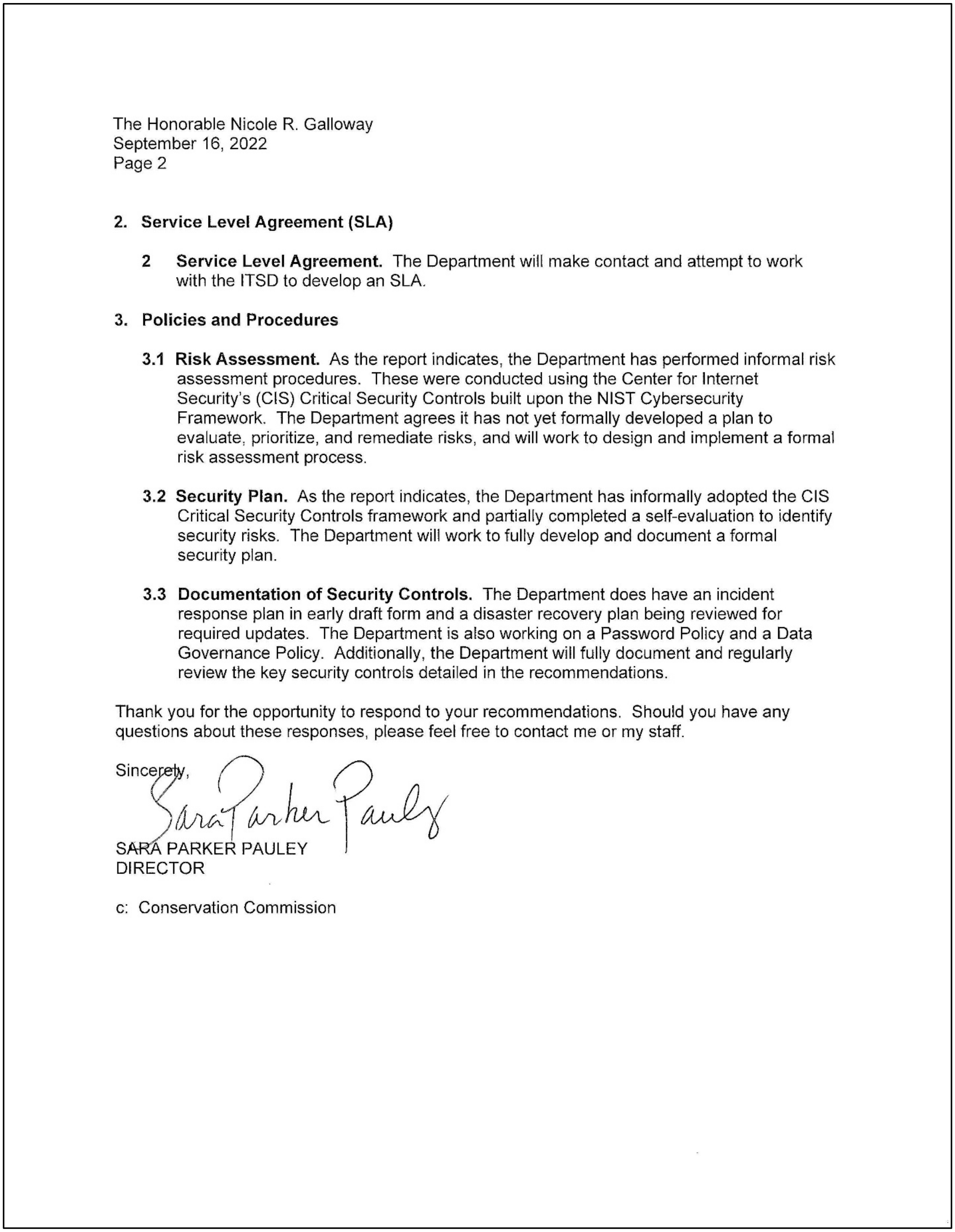
   1.2 **Password expiration.** The Department agrees with the recommendation and is currently working on reducing the number of these accounts while also working on establishing a policy and procedures to ensure user account passwords are consistently set to periodically expire.

   1.3 **Inactive user accounts.** The Department agrees with the recommendation and is currently reviewing unused accounts while also working on establishing a policy and procedures to ensure user accounts are periodically reviewed for lack of use.

   1.4 **Existing user access.** The Department agrees with the recommendation and is currently working on establishing a policy and procedures to ensure user access rights are periodically reviewed and remain appropriate and aligned with job responsibilities.

COMMISSION

MARGARET F. ECKELKAMP Washington	STEVEN D. HARRISON Rolla	MARK L. McHENRY Kansas City	WM. L. (BARRY) ORSCHELN Columbia



The Honorable Nicole R. Galloway
September 16, 2022
Page 2

2. Service Level Agreement (SLA)

2 **Service Level Agreement.** The Department will make contact and attempt to work with the ITSD to develop an SLA.

3. Policies and Procedures

3.1 Risk Assessment. As the report indicates, the Department has performed informal risk assessment procedures. These were conducted using the Center for Internet Security's (CIS) Critical Security Controls built upon the NIST Cybersecurity Framework. The Department agrees it has not yet formally developed a plan to evaluate, prioritize, and remediate risks, and will work to design and implement a formal risk assessment process.

3.2 Security Plan. As the report indicates, the Department has informally adopted the CIS Critical Security Controls framework and partially completed a self-evaluation to identify security risks. The Department will work to fully develop and document a formal security plan.

3.3 Documentation of Security Controls. The Department does have an incident response plan in early draft form and a disaster recovery plan being reviewed for required updates. The Department is also working on a Password Policy and a Data Governance Policy. Additionally, the Department will fully document and regularly review the key security controls detailed in the recommendations.

Thank you for the opportunity to respond to your recommendations. Should you have any questions about these responses, please feel free to contact me or my staff.

Sincerely,

Sara Parker Pauly

SARA PARKER PAULEY
DIRECTOR

c: Conservation Commission