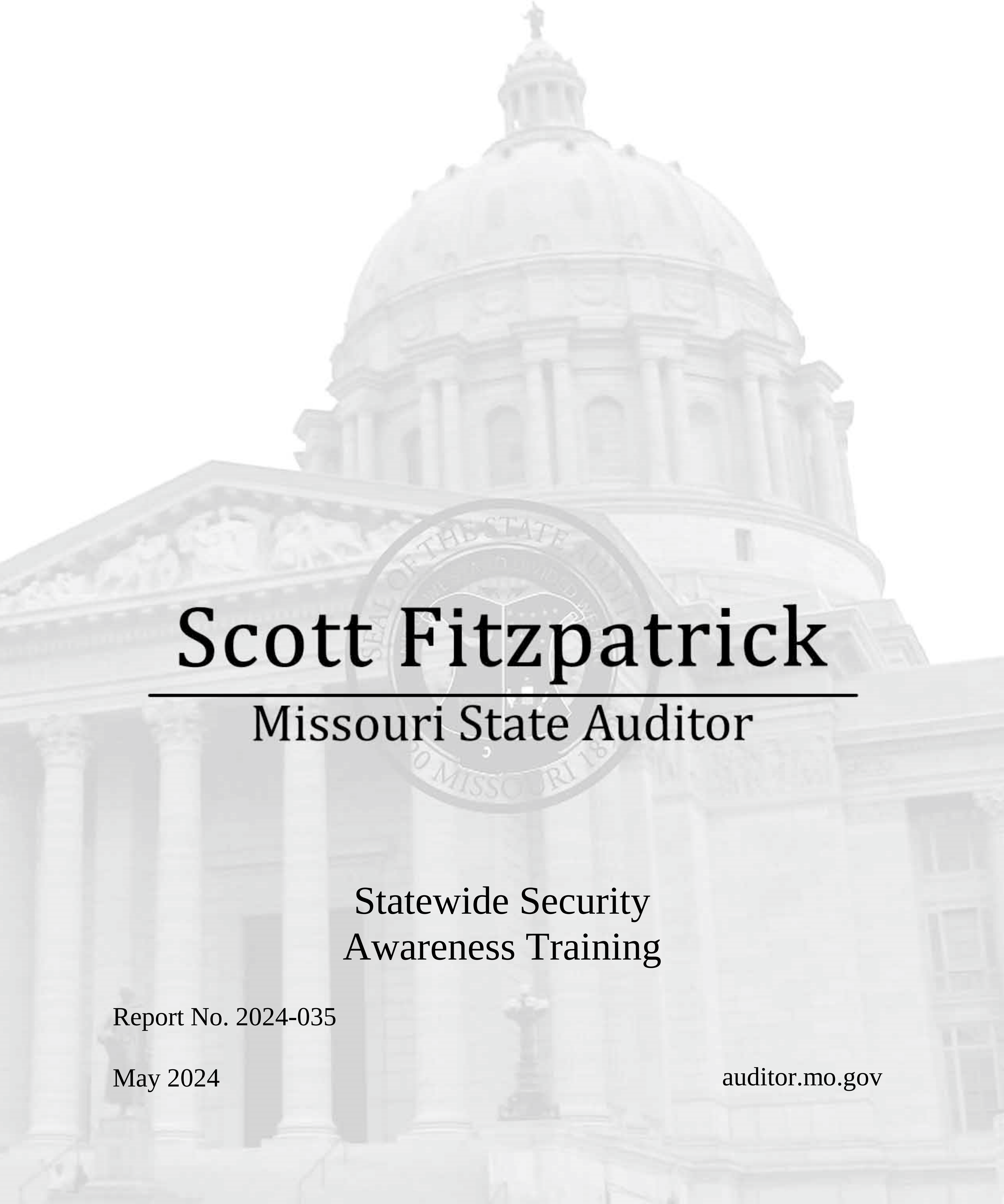


Scott Fitzpatrick

Missouri State Auditor

Statewide Security Awareness Training

Report No. 2024-035

May 2024

auditor.mo.gov

May 2024

Scott Fitzpatrick
Missouri State Auditor

CITIZENS SUMMARY

Findings in the audit of Statewide Security Training Awareness

Background

According to the Office of Administration Information Technology Services Division (ITSD), security awareness training is the basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. Security awareness training teaches employees how to protect information technology systems and agency data, and develops skills and knowledge, enabling employees to perform their jobs more securely. Security awareness training also improves the security posture of the enterprise [the state], and facilitates the implementation of appropriate security policies and procedures.

The ITSD was formed in January 2005 to consolidate information technology (IT) staff and funding. This consolidation primarily covered most executive branch agencies. The ITSD provides services, including security awareness training services, to its consolidated entities (CEs). Non-consolidated entities (NCEs), which are structurally independent of the ITSD, maintain their own internal IT departments that provide services, including security awareness training services, to their employees. Despite their structural independence, many NCEs remain in communication with, and sometimes enter into selective coordination with, the ITSD. The overall structure and distinct roles between the ITSD, CEs, and NCEs present general challenges to achieving statewide security awareness.

Scope and Methodology

The scope of our audit included, but was not limited to, the year ended June 30, 2023.

To evaluate the state's policies and procedures related to security awareness training, we reviewed written ITSD policies and procedures available, and interviewed the management of each NCE to understand their security awareness training activities. We also interviewed ITSD management on behalf of the CEs. We obtained all 18 CEs' training records for the 6 months ending June 30, 2023. To analyze results, we compared the training records to personnel records from the state's SAM II Human Resources system to determine the number of monthly security trainings each employee had completed during the 6-month test period. We limited our analysis to approximately 30,000 individuals who were actively employed, and remained with their CE, for the full 6 months. We performed procedures to ensure the data was complete to support our audit objectives, but reviewing internal controls of these systems was not part of our objectives.

To evaluate the ITSD's monitoring controls over security awareness training we interviewed ITSD management on behalf of the CEs, and identified and evaluated related policies and procedures.

Consolidated Entity Training Not Being Consistently Completed, Oversight Improvements Are Needed

CE employees did not consistently complete monthly security awareness training required by ITSD policy. A review of training results for the 6 months ending June 30, 2023, found approximately 20 percent of employees did not complete any of the 6 monthly trainings during that period, and 30 percent of employees received less than half of the required trainings in the test period.

Additionally, the ITSD does not provide oversight of the CEs' administration of cyber security awareness training. On May 1, 2023, the ITSD issued an updated security training policy with an additional clarification that "audits and assessments will be performed" by "authorized organizations" to help ensure compliance with the policy. However, this policy was rescinded by ITSD in June 2023 and has not been reissued, but is currently being reevaluated and is in draft form.

Based on our review of CE training records, most CEs have employees who were unofficially exempted, and thus, lacked the expected opportunities to receive and complete monthly security awareness training.

Non-Consolidated Entity Training and Phishing Testing Weaknesses

Four of 16 NCEs do not provide or obtain ongoing security awareness training for their employees. In addition, 9 of 16 NCEs do not perform or obtain phishing testing on their employees. Most of the remaining 7 NCEs contracted with vendors to perform phishing testing on their employees. The 4 NCEs that do not provide security awareness training to their employees are also included in the 9 entities that do not do phishing testing. As a result of these weaknesses, state resources such as data, systems, and/or monetary funds are at increased risk of loss or exposure.

Because of the nature of this audit, no rating is provided.

Statewide Security Awareness Training
Table of Contents

SCOTT FITZPATRICK
MISSOURI STATE AUDITOR

Honorable Michael L. Parson, Governor
and
Kenneth J. Zellers, Commissioner
Office of Administration
Jefferson City, Missouri

We have audited certain aspects of state security awareness training activities to determine if training is being provided to help users protect state resources such as data, systems and/or funds from loss or exposure. This audit was conducted in fulfillment of our duties under Chapter 29, RSMo. The objectives of our audit were to:

1. Evaluate the state's policies and procedures related to security awareness training.

2. Evaluate the Office of Administration Information Technology Services Division's (ITSD) monitoring controls over security awareness training.

Except as discussed in the following paragraph, we conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the 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 a reasonable basis for our findings and conclusions based on our audit objectives.

Generally accepted government auditing standards require us to obtain and report the views of responsible officials of the audited entity concerning the findings, conclusions, and recommendations included in the audit report. The entities referenced in Management Advisory Report (MAR) finding number 2 are not supported by a central agency that could respond broadly on the entities' behalf. Accordingly, for these audited entities, we obtained the views of responsible officials for the recommendation outlined in MAR finding number 2, but did not include them in the report.

For the areas audited, we identified (1) weaknesses in policies and procedures related to security awareness training, and (2) the need for improvement in the ITSD's monitoring controls over security awareness training. The accompanying Management Advisory Report presents our findings arising from our audit of statewide security awareness training. Generally accepted government auditing standards allow for information sensitive in nature to be omitted from public disclosure in certain instances. To avoid compromising the confidentiality of the sensitive information presented in this report, the names of individual agencies and entities have been omitted. Confidential communication has been made to the ITSD regarding which audit findings apply to which consolidated entities, and separate confidential communications were made to individual non-consolidated entities regarding any audit findings that apply to their respective entities.

Scott Fitzpatrick

Scott Fitzpatrick
State Auditor

Statewide Security Awareness Training Introduction

Background

According to the Office of Administration Information Technology Services Division (ITSD), security awareness training is the basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. Security awareness training teaches employees how to protect information technology systems and agency data, and develops skills and knowledge, enabling employees to perform their jobs more securely. Security awareness training also improves the security posture of the enterprise [the state], and facilitates the implementation of appropriate security policies and procedures.[1]

Security incidents can often be traced to a user error, such as clicking on a link in a malicious email, or sharing account credentials with bad actors. It is important for the state to establish a security culture that takes threats seriously and teaches employees how to protect state resources.

Consolidation

The ITSD was formed in January 2005 to consolidate information technology (IT) staff and funding. This consolidation primarily covered most executive branch agencies. The ITSD provides services, including security awareness training services, to its consolidated entities (CEs).[2]

Non-consolidated entities (NCEs), which are structurally independent of the ITSD, maintain their own internal IT departments that provide services, including security awareness training services, to their employees. Despite their structural independence, many NCEs remain in communication with, and sometimes enter into selective coordination with, the ITSD.

The table below summarizes the count of CEs and NCEs, and the count of employees in each:

Consolidated and Non-Consolidated Entities, June 30, 2023

	Entity Count	Employee Count
Consolidated	18	37,020
Non-Consolidated*	17	14,699
Total	35	51,719

* This count includes the State Auditor's Office. The State Auditor's Office was excluded from the analysis of NCEs later in this report to ensure we remained independent on this audit. See MAR finding number 2.

Source: Entity counts were provided by the ITSD. Employee counts are from the SAM II Human Resources system for most entities. Entity management provided the data for the remaining entities not maintained in SAM II.

[1] ITSD, Missouri Adaptive Enterprise Architecture, Security Awareness Training, May 2019, <https://oa.mo.gov/sites/default/files/TA-Security-Awareness-Training.pdf>, accessed July 20, 2023.

[2] For purposes of this report, an individual entity may be an agency, specific division(s) of an agency, or a quasi-governmental agency affiliated with the state of Missouri.

The overall structure and distinct roles between the ITSD, CEs, and NCEs present general challenges to achieving statewide security awareness.

According to the National Institute of Standards and Technology (NIST),[3] 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. 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[4] while ISACA[5] states cybersecurity encompasses all that protects enterprises and individuals from intentional attacks, breaches, and incidents as well as the consequences.[6] 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.

Scope and Methodology

The scope of our audit included, but was not limited to, the year ended June 30, 2023.

To evaluate the state's policies and procedures related to security awareness training, we reviewed written ITSD policies and procedures available, and interviewed the management of each NCE[7] to understand their security awareness training activities. We also interviewed ITSD management on behalf of the CEs. We obtained all 18 CEs' training records for the 6 months

[3] 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 October 2, 2023.

[4] 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 October 2, 2023.

[5] ISACA is an international professional association, formerly known as the Information Systems Audit and Control Association, that is focused on IT governance.

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

[7] The State Auditor's Office (SAO) is an NCE. However, to ensure we remained independent in all aspects of this audit, the SAO was excluded from consideration during the audit.

ending June 30, 2023. To analyze results, we compared the training records to personnel records from the state's SAM II Human Resources system (SAM II) to determine the number of monthly security trainings each employee had completed during the 6-month test period. We limited our analysis to approximately 30,000 individuals who were actively employed, and remained with their CE, for the full 6 months. We performed procedures to ensure the data was complete to support our audit objectives, but reviewing internal controls of these systems was not part of our objectives.

To evaluate the ITSD's monitoring controls over security awareness training we interviewed ITSD management on behalf of the CEs, and identified and evaluated related policies and procedures.

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)
- ISACA

1. Consolidated Entity Training Not Being Consistently Completed, Oversight Improvements Are Needed

Consolidated entity (CE) employees did not consistently complete monthly security awareness training required by Office of Administration Information Technology Services Division (ITSD) policy. Based on our review of training data, approximately 20 percent of employees did not complete any security awareness training during our test period. As a result, state resources such as data, systems and/or funds are at increased risk of exposure or loss. This condition had not been detected, in part, due to ITSD policy not requiring the ITSD or the CEs to monitor the completion of security awareness training.

The ITSD contracts with a vendor to obtain monthly security awareness training content in the form of interactive videos lasting approximately 5 to 10 minutes. Records of which CE employees completed these monthly trainings are uploaded to an electronic training administration system, and can be accessed by each CE's authorized personnel. The ITSD can directly access training records for most CEs, or in limited situations, can request them from the CEs.

Training not being consistently completed

We reviewed training results for the 6 months ending June 30, 2023, and found approximately 20 percent of employees did not complete any of the 6 monthly trainings during that period, and 30 percent of employees received less than half of the required trainings in the test period.

We obtained all 18 CEs' training records for the 6 months ending June 30, 2023, and compared them to personnel records from the state's Human Resources system (SAM II) to determine the percentage of employees completing assigned trainings. We limited our analysis to approximately 30,000 individuals who were actively employed, and remained with the same CE, for the full 6-month period.[8]

Table 1 on the following page shows the percentage of employees completing the monthly trainings during the 6 months ended June 30, 2023, for each anonymized CE. For example, 86 percent of Entity A employees completed all 6 of the monthly trainings, 7 percent completed 5 of the monthly trainings, and so on. The table also presents, for all employees in a given CE, the weighted average number of monthly trainings completed, with 6.0 (6 months) being the maximum possible value.

[8] We applied this limitation to reach fair and consistent results across all 18 CEs and within the 6-month period. For example, we removed individuals not employed for the entire 6-month period because certain factors and data limitations may unfairly and negatively skew results.

Table 1: Consolidated Entity Monthly Training Completion Results for the 6 Months Ended June 30, 2023

Entity	Exempt and 0 Months[1]	0 Months Completed	1 Month Completed	2 Months Completed	3 Months Completed	4 Months Completed	5 Months Completed	6 Months Completed	Weighted Average Months Completed
Entity A	1%	0%	0%	1%	1%	4%	7%	86%	5.7
Entity B	1%	4%	2%	1%	2%	2%	5%	83%	5.4
Entity C	5%	0%	1%	2%	4%	8%	11%	69%	5.2
Entity D	2%	4%	2%	4%	5%	7%	15%	61%	5.0
Entity E	2%	12%	3%	4%	5%	8%	14%	52%	4.4
Entity F	1%	11%	6%	5%	5%	9%	13%	50%	4.3
Entity G	1%	17%	4%	4%	5%	7%	12%	50%	4.2
Entity H	21%	6%	1%	2%	2%	3%	8%	57%	4.1
Entity I	1%	13%	7%	5%	6%	11%	13%	44%	4.1
Entity J	1%	14%	6%	5%	7%	9%	13%	45%	4.0
Entity K	2%	22%	4%	6%	7%	6%	16%	37%	3.6
Entity L	2%	24%	6%	3%	5%	10%	9%	41%	3.6
Entity M	0%	42%	4%	8%	0%	0%	8%	38%	2.9
Entity N	1%	41%	6%	5%	5%	6%	9%	27%	2.6
Entity O	56%	0%	0%	0%	0%	0%	6%	38%	2.6
Entity P	1%	64%	6%	4%	3%	4%	5%	13%	1.4
Entity Q	78%	0%	0%	0%	4%	0%	9%	9%	1.1
Entity R[2]	0%	98%	1%	0%	0%	0%	0%	1%	0.0
Average for all CEs[3]	**3%**	**21%**	**3%**	**3%**	**4%**	**6%**	**9%**	**51%**	**4.0**

[1] These individuals were exempted, meaning they were not entered in a training system, and have no available training data. Therefore, these individuals lacked the expected opportunities to receive and complete monthly security awareness training.
[2] According to the ITSD, a technical issue prevented most individuals at this entity from being able to access the training.
[3] This row's values were calculated using the count of individuals across all CEs. Thus, this row's values are not an average of the preceding numbers in each respective column.

Source: SAO analysis of consolidated entities' training data and the SAM II Human Resources system data.

Lack of Oversight

The ITSD does not provide oversight of the CEs' administration of cyber security awareness training. Effective September 2007, the ITSD policy over security awareness training for CEs requires all CE users who use state-owned systems to complete monthly cyber security awareness training. In addition, this policy requires all cyber security awareness training be documented by the CE, but does not include any requirements for the CE or ITSD to monitor the implementation of the policy. On May 1, 2023, the ITSD issued an updated security training policy with an additional clarification that "audits and assessments will be performed" by "authorized organizations" to help ensure compliance with the policy.[9] However, this policy was rescinded[10] by the ITSD in June 2023 and has not been reissued, but is currently being reevaluated and is in draft form. Based on discussions with ITSD personnel, the ITSD had not obtained or reviewed CE training records, such as those presented in Table 1, prior to our July 2023 request for such records.

Exempting some employees from cyber security training requirements is not allowed by policy

Based on our review of CE training records, most CEs have employees who were unofficially exempted, and thus, lacked the expected opportunities to receive and complete monthly security awareness training. This is especially significant for CEs Q (78 percent of employees), O (56 percent of employees), and H (21 percent of employees). However, current ITSD policy requires all CE users who use state-owned systems to complete monthly cyber security awareness training and does not address or discuss that any employees may be exempted from security awareness training.

Recommendation

The ITSD update its security awareness training policy to require oversight procedures for CE security awareness training to ensure required trainings are being completed, and clarify whether CEs are allowed to exempt certain employees from training requirements.

Auditee's Response

The ITSD's written response indicates it agrees with this recommendation. The ITSD's full response is included as Appendix A.

2. Non-Consolidated Entity Training and Phishing Testing Weaknesses

Four of 16 non-consolidated entities (NCEs)[11] do not provide or obtain ongoing security awareness training for their employees. In addition, 9 of 16 NCEs do not perform or obtain phishing testing on their employees. The 4 NCEs that do not provide security awareness training to their employees are also included in the 9 entities that do not do phishing testing. As a result of these weaknesses, state resources such as data, systems, and/or monetary funds are at increased risk of loss or exposure.

Training not provided

Four of 16 NCEs do not provide or obtain ongoing security awareness training for their employees. Reasons for not providing security training varied across these entities, including decisions made by previous administrations, technical difficulties accessing the ITSD's training system, and budget limitations. These reasons reflect a general lack of priority of such training.

[9] ITSD Office of Cyber Security, Policy OCS-001003, *Information Security Awareness, Training, and Education Policy*, May 2023

[10] According to ITSD officials, this policy was rescinded because it was issued without proper Office of Administration management approval.

[11] The State Auditor's Office was excluded from this analysis to ensure we remained independent on this audit, and therefore, is not included in the count of NCEs in the report.

The remaining 12 NCEs either created their own training content, or contracted for the training. Some leveraged the same vendor and contract used by the ITSD for its CEs. Others preferred different vendors for their own unique operational, technical, and/or budgetary considerations.

The 16 NCEs are individually responsible for all information technology-related decisions and tasks to support their operations and employees. Although the NCEs are structurally independent from the ITSD, many NCEs remain in communication with (and sometimes enter selective coordination with) the ITSD to obtain knowledge and enhance operations. The ITSD makes itself available to NCEs for consulting and direct support.

The NCEs are not required to follow ITSD policy or leverage its efforts. However, ITSD's existing cyber security training policy for CEs appears to be an appropriate starting point for NCEs when developing policies for their respective entities.

Phishing testing not performed

Nine of 16 NCEs do not perform phishing[12] testing on their employees as recommended by the National Institute of Standards and Technology (NIST). According to the NIST, entities should employ techniques to increase the security awareness of users, which could include practical social engineering exercises like phishing testing to "collect information, gain unauthorized access, or simulate the adverse impact of opening malicious email attachments."[13] Phishing is a common cybercrime that can result in identity theft, financial loss, and/or data exposure. Employers, either directly or through vendors, can perform phishing testing on employees to securely simulate real phishing, improve the entity's resilience, and detect additional training needs.

Entities not performing phishing testing provided several flawed reasons for not performing such testing. One entity cited the use of preventive controls, such as email filtering, and believed such controls made phishing testing unnecessary. However, while such controls can support employee-involved security awareness efforts, they are not a replacement for them. Several entities also expressed an incorrect belief that the ITSD would not provide phishing testing to NCEs. However, based on discussions with ITSD

[12] Phishing is a cybercrime in which a target or targets are contacted by email, telephone, or text message by a phisher, who is someone posing as a legitimate contact or institution. The phisher lures targets, often by creating a sense of urgency, into providing sensitive data such as personally identifiable information, passwords, and/or financial details. The phisher then uses the information to access important accounts and/or perform other unauthorized actions that can circumvent the target's existing internal controls.

[13] NIST, Special Publication 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, p. 60-61, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>, accessed December 4, 2023.

personnel, NCEs are welcome to leverage its phishing testing efforts. This may reflect a no cost option that resolves another entity's concern over budget limitations.

Most of the remaining 7 NCEs contracted with vendors to perform phishing testing on their employees.

Recommendation

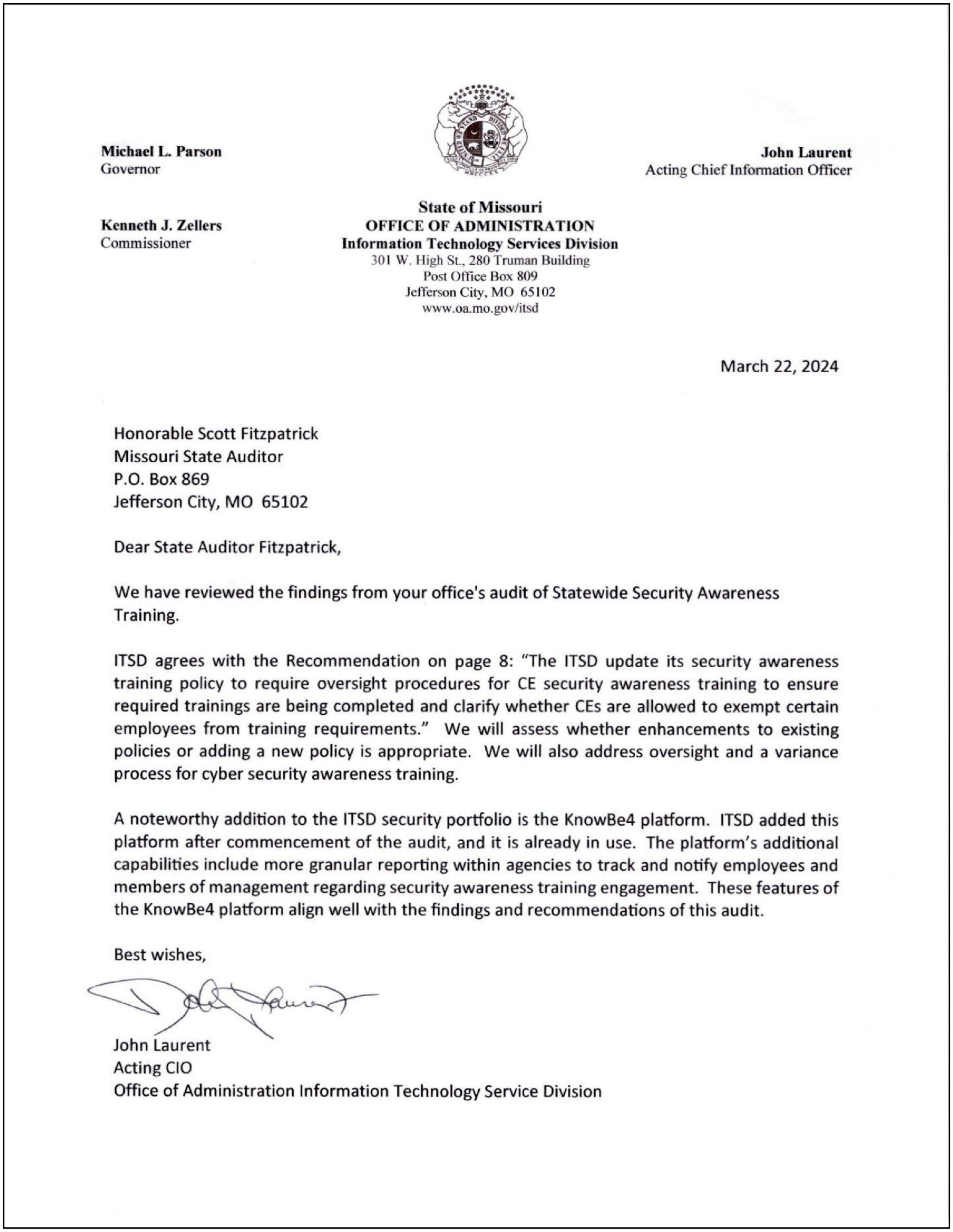
NCEs not performing security awareness training and phishing testing should consider the ITSD's security awareness training policy and phishing testing efforts and establish policies and procedures to ensure training and testing are completed regularly for their employees. NCEs not currently providing security training or phishing testing should consider using ITSD as a resource to implement such procedures.

Auditee's Response

Due to the nature of this finding, and to preserve the anonymity of the relevant NCEs, we will not present the views of responsible officials for this recommendation.

Although the ITSD is not the responsible official for this finding, we also discussed the finding with the ITSD. The ITSD expressed interest in assisting the NCEs, and reaffirmed the NCEs are welcome to leverage its security awareness training and phishing testing efforts. This general discussion did not specify terms, make guarantees, or change the degrees of authority between the ITSD and the NCEs.

Appendix
Statewide Security Awareness Program
Office of Administration Responses to Audit Recommendations



Michael L. Parson
Governor

Kenneth J. Zellers
Commissioner

John Laurent
Acting Chief Information Officer

State of Missouri
OFFICE OF ADMINISTRATION
Information Technology Services Division
301 W. High St., 280 Truman Building
Post Office Box 809
Jefferson City, MO 65102
www.oa.mo.gov/itsd

March 22, 2024

Honorable Scott Fitzpatrick
Missouri State Auditor
P.O. Box 869
Jefferson City, MO 65102

Dear State Auditor Fitzpatrick,

We have reviewed the findings from your office's audit of Statewide Security Awareness Training.

ITSD agrees with the Recommendation on page 8: "The ITSD update its security awareness training policy to require oversight procedures for CE security awareness training to ensure required trainings are being completed and clarify whether CEs are allowed to exempt certain employees from training requirements." We will assess whether enhancements to existing policies or adding a new policy is appropriate. We will also address oversight and a variance process for cyber security awareness training.

A noteworthy addition to the ITSD security portfolio is the KnowBe4 platform. ITSD added this platform after commencement of the audit, and it is already in use. The platform's additional capabilities include more granular reporting within agencies to track and notify employees and members of management regarding security awareness training engagement. These features of the KnowBe4 platform align well with the findings and recommendations of this audit.

Best wishes,

John Laurent
Acting CIO
Office of Administration Information Technology Service Division