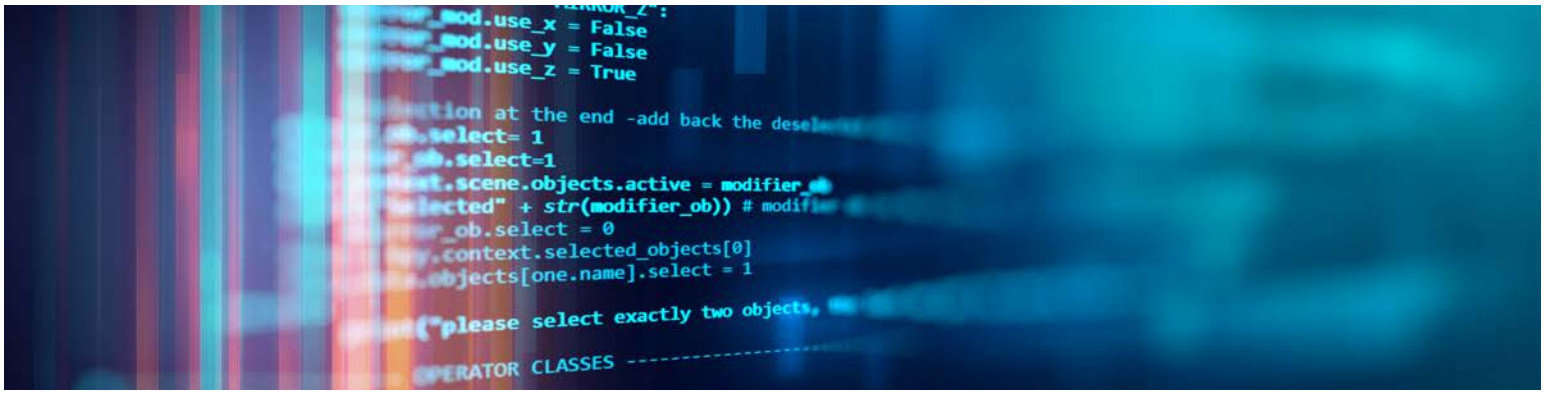
Gaps in Oversight Contribute to Weaknesses in the State's Information Security

High Risk Update—Information Security

July 2019

REPORT 2018-611



CALIFORNIA STATE AUDITOR
621 Capitol Mall, Suite 1200 | Sacramento | CA | 95814

916.445.0255 | TTY **916.445.0033**

For complaints of state employee misconduct,
contact us through the **Whistleblower Hotline**:
1.800.952.5665

Don't want to miss any of our reports? Subscribe to our email list at **auditor.ca.gov**

For questions regarding the contents of this report, please contact Margarita Fernández, Chief of Public Affairs, *at* 916.445.0255

July 16, 2019
2018-611

The Governor of California
President pro Tempore of the Senate
Speaker of the Assembly
State Capitol
Sacramento, California 95814

Dear Governor and Legislative Leaders:

This report presents the results of our high risk audit regarding weaknesses in the State's information security. While we previously found that the California Department of Technology (technology department) has made strides toward improving its oversight, and the state entities it oversees have increased their compliance with established security standards, state entities that fall outside the technology department's purview need to do more to safeguard the information they collect, maintain, and store. State law generally requires state entities within the executive branch that are under the Governor's direct authority (reporting entities) to comply with the information security and privacy policies that the technology department prescribes and to annually report to the technology department on their compliance. However, state law does not apply the technology department's policies and procedures to entities that fall outside of that authority (nonreporting entities), such as constitutional offices and those in the judicial branch. Consequently, gaps in oversight have contributed to weaknesses in nonreporting entities' information security statuses.

We surveyed 33 nonreporting entities from around the State and reviewed 10 of them in detail. Twenty-nine of the 33 obtained an information security assessment to evaluate their compliance with the specific security standards they selected, 24 learned that they were only partially compliant, and 21 identified high-risk deficiencies. Further, nonreporting entities may be unaware of other information security weaknesses because many of them have relied upon assessments that were limited in scope. For example, five of the 10 nonreporting entities we reviewed had assessed only a portion of their selected standards, and one had neither adopted any standards nor performed any assessments.

Although nonreporting entities are not subject to the technology department's policies and procedures, some are subject to an oversight framework that requires them to assess their information security regularly. This was the case for three of the four entities that had fully assessed their selected standards, leading us to conclude that external oversight improves a state entity's information security status. Accordingly, we recommend that the Legislature amend state law to require all nonreporting entities to obtain or perform comprehensive information security assessments at least every three years and to confidentially submit certifications of their compliance to the Legislature.

Respectfully submitted,

Elaine M. Howle

ELAINE M. HOWLE, CPA
California State Auditor

Blank page inserted for reproduction purposes only.

Contents

Blank page inserted for reproduction purposes only.

Summary

Results in Brief

Gaps in oversight weaken the State's efforts to keep its information secure. Although we previously found that the California Department of Technology (technology department) has made progress in its oversight since our initial 2013 assessment, and the state entities subject to its oversight have increased their compliance with established standards, state entities that do not fall under the purview of the technology department need to do more to safeguard the information they collect, maintain, and store. State law generally requires state entities within the executive branch under the Governor's direct authority (reporting entities) to comply with information security and privacy policies that the technology department prescribes. However, state law does not apply the technology department's policies and procedures to entities that fall outside of that authority (nonreporting entities).

We surveyed 33 nonreporting entities from around the State and reviewed 10 of them in detail. Most of the 33 surveyed entities asserted that they had selected one or more standards to use in developing their information security policies. In addition, 29 of the 33 entities said they performed a self-assessment or contracted with an independent assessor to evaluate their compliance with the specific standards they selected. However, 24 of the assessments concluded that the respective entities were only partially compliant. In addition, 21 of those assessments identified high-risk deficiencies.

The nonreporting entities we surveyed may be unaware of additional information security weaknesses because many of them relied upon information security assessments that were limited in scope. For example, five of the 10 nonreporting entities we reviewed had assessed only a portion of their selected security standards, which limits their ability to identify potential vulnerabilities, and one had neither adopted any security standards nor performed any assessments. Although nonreporting entities are not subject to the technology department's policies and procedures, some are subject to an oversight framework that requires them to assess their information security regularly. This was the case for three of the four entities that had fully assessed their selected standards, leading us to conclude that external oversight improves a state entity's information security status. At the same time, nonreporting entities without external oversight that fail to routinely assess their level of compliance with adopted security standards and then fail to address identified deficiencies are placing some of the State's sensitive data at risk of unauthorized use, disclosure, or disruption.

Audit Highlights . . .

Our high risk audit regarding nonreporting entities' compliance with security standards revealed the following:

» *State entities that do not fall under the purview of the technology department need to do more to safeguard the information they collect, maintain, and store.*

- *Of the 33 nonreporting entities surveyed, 29 obtained an information security assessment to evaluate their compliance with the security standards they selected.*
- *Twenty-four nonreporting entities were only partially compliant and nearly all had high-risk deficiencies.*

» *Nonreporting entities may be unaware of other information security weaknesses because many of them relied upon assessments that were limited in scope.*

- *Five of the 10 nonreporting entities we reviewed had assessed only a portion of their selected security standards, and one had neither adopted any security standards nor performed any assessments.*

» *Some nonreporting entities are subject to an oversight framework that requires them to assess their information security regularly.*

- *Three of the four nonreporting entities that fully assessed their selected standards were subject to such oversight, leading us to conclude that external oversight improves a state entity's information security status.*

Recommendations

To strengthen the information security practices of nonreporting entities, the Legislature should amend state law to do the following:

- Require all nonreporting entities to adopt information security standards comparable to the information security and privacy policies prescribed by the technology department.
- Require all nonreporting entities to obtain or perform comprehensive information security assessments no less frequently than every three years to determine compliance with the entirety of their adopted information security standards.
- Require all nonreporting entities to confidentially submit certifications of their compliance with their adopted standards to the Assembly Privacy and Consumer Protection Committee and, if applicable, to confidentially submit corrective action plans to address any outstanding deficiencies.

Introduction

Background

Numerous retailers, financial institutions, and government agencies have reported data security incidents that compromised the integrity, confidentiality, or availability of their information, some of which resulted in the disclosure of that information to unauthorized parties. For example, in 2017 a nationwide consumer reporting agency suffered a data breach involving the personal information of more than 145 million Americans. In 2016 the Securities and Exchange Commission experienced a breach of its database that stores corporate disclosures, resulting in unauthorized access to nonpublic information.

California's *State Administrative Manual* (SAM) describes the State's information assets, including its data processing capabilities, information technology infrastructure, and data, as an essential public resource. In fact, for many state entities, program operations would effectively cease in the absence of key computer systems, and in some cases, the failure or disruption of a system would immediately jeopardize public health and safety. If state information systems and resources should become unavailable, this could potentially have a detrimental impact on the state economy and on the residents who rely on state programs.

In addition to disrupting the State's ability to operate, data breaches have significant financial costs. According to a 2018 report published by IBM Security and the Ponemon Institute, the average total cost of a data breach in 2017 was $3.86 million.[1] However, the report noted that larger breaches of 50 million records or more can cost $350 million on average. Given the amount of data the State maintains, the financial cost of a data breach and the damage to its credibility and reputation could be significant. Moreover, a breach involving disclosure of personal information could be detrimental to residents if, for example, an unauthorized person acquired that information and used it to commit identity theft.

The consequences of a data breach highlight the importance of information security in both the public and private sectors. *Information security* refers to protecting information, information systems, equipment, software, and people from a wide spectrum of threats and risks. Implementing appropriate security measures and controls is critical to ensuring the confidentiality, integrity, and availability of both the information and the information systems that state entities need to accomplish their missions, fulfill their legal responsibilities, and maintain their day-to-day operations.

[1] Ponemon Institute, *2018 Cost of a Data Breach Study: Global Overview*, IBM, July 2018.

Information security is also the means by which state entities can protect the privacy of the personal information they hold, such as their employees' Social Security numbers and home addresses.

Information Security Roles and Responsibilities

The California Department of Technology (technology department) is responsible for providing direction for the State's information security. State law generally requires state entities within the executive branch that are under the Governor's direct authority (reporting entities) to comply with the information security practices that the technology department prescribes and to annually report to the technology department on their compliance with these practices. However, state law does not apply the technology department's policies and procedures to entities that fall outside of the Governor's direct authority (nonreporting entities), such as constitutional offices and those in the judicial branch.

State law and SAM require reporting entities to perform risk assessments and independent information security assessments. Specifically, SAM requires reporting entities to conduct a comprehensive risk assessment every two years to evaluate their risk management strategy and to perform periodic vulnerability scanning and penetration testing. In addition, state law permits the California Military Department (military department) to perform independent assessments. State law also requires entities to provide the technology department with the results of these assessments.

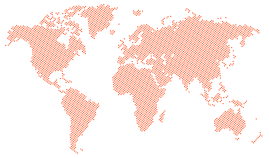
Information security falls within the scope of the Assembly Privacy and Consumer Protection Committee (Privacy Committee) and the Assembly Select Committee on Cybersecurity (Cybersecurity Committee). The Privacy Committee has jurisdiction over matters related to privacy, the protection of personal information, the security of data, and information technology, among others. It is also responsible for oversight of the technology department. The purpose of the Cybersecurity Committee is to examine information security vulnerabilities, assess resources, examine current cybersecurity policy for state networks, and develop partnerships to manage and respond to threats.

Information Security Standards

State law provides the technology department with the responsibility and authority to create, issue, and maintain policies, standards, and procedures governing information security for state agencies. Chapter 5300 of SAM (SAM 5300) provides the security and privacy policy standards with which reporting entities must comply and

notes that the State has adopted the National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) as its minimum information security control requirements. NIST 800-53 provides security and privacy controls for federal information systems and organizations. In addition to the state and federal government standards, certain international standards for information security may also be applied to organizations. Nonreporting entities may also be subject to industry-specific information security requirements. For example, some health care programs follow federal privacy and information security-related requirements, such as the Health Insurance Portability and Accountability Act of 1996. Moreover, some nonreporting entities choose to adopt one or more standards to address their specific needs. Although multiple standards for information security exist, the standards most commonly used by the 33 nonreporting entities we reviewed are SAM 5300, NIST 800-53, and information security standards established in the International Organization for Standardization and the International Electrotechnical Commission 27000 family of standards (ISO/IEC 27000 family). Figure 1 describes these standards.

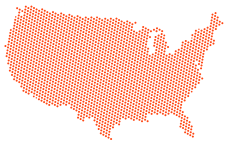
Figure 1
Information Security Standards



International Organization for Standardization/ International Electrotechnical Commission

ISO/IEC 27000 family

Requirements are generic and intended to be applicable to all organizations, regardless of type, size, or nature.



National Institute of Standards and Technology

NIST 800-53

Federal government standards, which may be adopted by nonfederal entities.

Technology Department

SAM 5300

Adopted NIST 800-53 as minimum information security control requirements and adopted additional standards that are maintained in the *Statewide Information Management Manual*. Only state entities within the executive branch that are under the Governor's direct authority are required to follow these standards.

Source: ISO/IEC 27000 family, NIST 800-53, and SAM 5300.

Although they are not required to follow SAM 5300, many nonreporting entities have adopted these or other comparable standards. Standards provide requirements for establishing, implementing, maintaining, and continually improving an entity's information security management system. The entity's needs and

objectives, its security requirements, the organizational processes it uses, and its size and structure influence how it establishes and implements such a system. The ISO/IEC 27000 family notes that all of these influencing factors are expected to change over time, which means that all entities should regularly evaluate their information security needs.

Regardless of which standards nonreporting entities choose to adopt, each of the standards addresses similar control areas, such as those described in Figure 2. For example, as we discuss earlier, SAM 5300 instructs reporting entities to use NIST 800-53 as the minimum information security control requirements for reporting entities, but it adopts additional standards and procedures to address more specific requirements or needs unique to California. These additional standards are maintained in the *Statewide Information Management Manual*. In addition, NIST 800-53 includes a section that shows how its security controls map to comparable security controls in the ISO/IEC 27000 family, demonstrating how the two standards align. When they adopt standards, nonreporting entities make it possible for internal and external parties to assess their ability to meet the information security requirements they have established.

Figure 2
Five Key Control Areas of Information Security Standards

Source: ISO/IEC 27000 family, NIST 800-53, and SAM 5300.

Information Security Is a High-Risk Issue

We previously reported on the deficiencies we identified in the security controls that state agencies have implemented over their information systems. The pervasiveness of these deficiencies led us to designate the technology department's oversight of information security as a high-risk issue. State law authorizes the California State Auditor (State Auditor) to develop a program for identifying, auditing, and reporting on high-risk state agencies and statewide issues. We first identified information security as a high-risk issue in our September 2013 audit report *High Risk: The California State Auditor's Updated Assessment of High-Risk Issues the State and Selected State Agencies Face*, Report 2013-601. The report concluded that the technology department was performing limited reviews to assess the security controls that reporting entities had implemented for their information systems; it also discussed the deficiencies in such controls that we noted at two of the reporting entities we audited.

Two years later, in our August 2015 follow-up report, *High Risk Update—Information Security: Many State Entities' Information Assets Are Potentially Vulnerable to Attack or Disruption*, Report 2015-611, we found that few of the state entities under the oversight of the technology department had fully complied with the State's mandated information security and privacy policies, standards, and procedures. For example, when we performed compliance reviews of selected information security requirements at five reporting entities, we found that each had deficiencies. Similarly, our survey of reporting entities for that report showed that 73 of the 77 respondents reported that they had yet to achieve full compliance with the State's requirements. We also observed that a significant number of entities—such as constitutional offices and those in the judicial branch—are not subject to the technology department's security standards. Given the significant findings we identified in our August 2015 report and the pervasiveness of the information security issues that we identified in previous reports—including significant deficiencies we discovered in the controls that two nonreporting entities had implemented over their information systems—we stated our intent in that report to assess the information security risks associated with nonreporting entities.

Finally, we included an update to this high-risk issue in our January 2018 audit report *High Risk: The California State Auditor's Updated Assessment of High-Risk Issues the State and Select State Agencies Face*, Report 2017-601. In that update, we reported that although information security remains a high-risk issue to the State, the technology department has made progress in its oversight, and reporting entities have increased their compliance

with SAM 5300. We also reiterated that the information security practices of state entities outside the purview of the technology department might warrant further investigation in the future. The information security status for such nonreporting entities is the subject of this report.

Audit Results

Nonreporting Entities Have Weaknesses in Their Information Security

Numerous weaknesses exist in the information security practices of many of the nonreporting state agencies that we surveyed and reviewed.[2] For example, 24 of the 33 nonreporting entities we surveyed indicated that they were only partially compliant with their selected information security standards. In addition, while those 24 had obtained information security assessments to identify deficiencies, some lack a framework to help them resolve the deficiencies. Moreover, because many of the assessments were limited in scope, we are concerned that nonreporting entities may be unaware of additional weaknesses in their information security.

Many Nonreporting Entities Identified Deficiencies in Their Information Security Programs

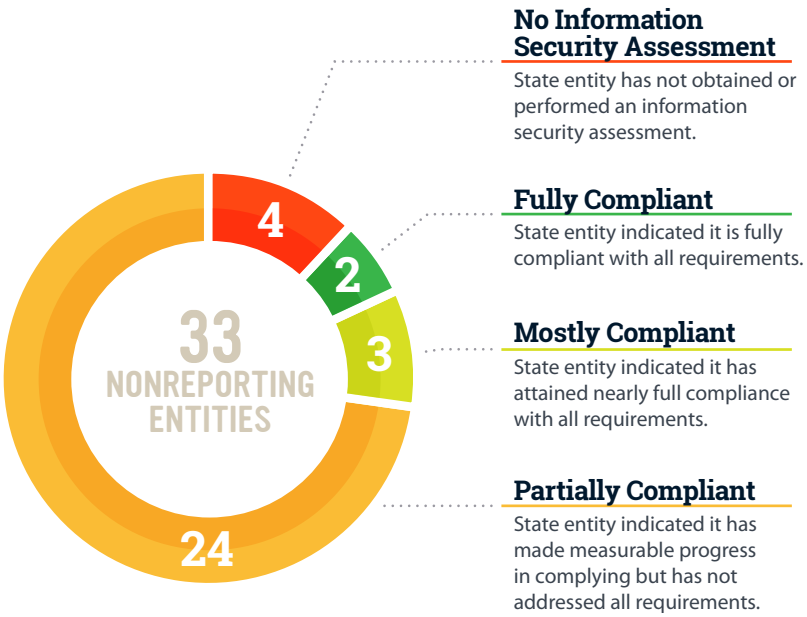
Our survey of nonreporting entities indicated that most of them are not adequately addressing information security. Twenty-nine of the 33 nonreporting entities we surveyed had obtained an information security assessment, and 24 learned they were only partially compliant with their selected standard, as shown in Figure 3. Of the remaining five nonreporting entities that conducted assessments, two were fully compliant and three were mostly compliant with their selected standard. The remaining four nonreporting entities had not performed an assessment, and in fact, three of them currently have no plans to proceed with an assessment. Without performing information security assessments, entities are likely unaware of whether their controls are implemented correctly and operating as intended.

The assessments of 21 nonreporting entities that were partially compliant with their selected standards identified high-risk deficiencies in their information security. Although the definition of *high risk* may vary among the information security standards used in performing a security assessment, risk is often calculated by considering threats or vulnerabilities and their associated impacts and likelihood of occurrence. For example, one entity failed to apply security updates to some of its devices, which poses the threat that known vulnerabilities in these devices could be exploited. Although nonreporting entities with partial compliance had high-risk deficiencies in various areas, the most common area was

[2] We surveyed 33 nonreporting entities from around the State and reviewed 10 of them in detail. To protect the State's information assets, we are not disclosing the names of the entities that we surveyed or reviewed. Instead, we assigned each of these entities a letter that we use throughout the report.

information security program management, that is, developing and maintaining an organizationwide program to protect information assets from identified risks. Findings within this area further highlight the weaknesses in the information security programs of nonreporting entities.

Figure 3
Entities' Compliance With Their Selected Standards



Source: Analysis of survey responses.

Some Nonreporting Entities Have Failed to Resolve Known Deficiencies

Despite being aware of significant deficiencies in their current information security programs, some nonreporting entities have been slow to address these weaknesses. Although two of the 24 nonreporting entities with partial compliance asserted that they had resolved the high-risk deficiencies identified in their most recent assessment, 11 entities stated that they would need another three years to resolve the deficiencies. In addition, when we followed up with a selection of the nonreporting entities, we found that some did not have an adequate process or time frame for resolving their deficiencies.

Some nonreporting entities have failed to implement effective processes for prioritizing and tracking their remediation efforts.

Some of the nonreporting entities we reviewed have failed to implement effective processes for prioritizing and tracking their remediation efforts. The technology department requires reporting entities to develop a plan of action and milestones for all security compliance deficiencies and for all significant information security risks that they cannot immediately address. Reporting entities use the plan of action and milestones to communicate details about remediating each deficiency to the technology department. Reporting entities are also typically required to provide quarterly updates to the technology department on their progress toward completion of the plans. However, because nonreporting entities are not subject to this requirement, some have chosen a more informal process for addressing their deficiencies.

For example, in December 2017, the military department identified 16 findings at Entity A. One of these findings noted that Entity A failed to change the default password for certain information security systems, which poses a significant threat of an attacker gaining unauthorized access to its network. Although the military department identified five top areas of significant concern for Entity A to address, as of March 2019; Entity A had not fully addressed any of those areas. Moreover, as of April 2019, nearly 16 months after Entity A received its independent information security assessment, it had yet to determine the scope, schedule, funding, and staffing required to implement the remediation strategy for some of its findings. By failing to identify a remediation strategy and by failing to perform a timely assessment of its resource needs to implement the strategy, Entity A risks further delays in resolving its outstanding deficiencies.

Another entity we reviewed has not adequately documented a plan for remediating its existing findings. Specifically, although Entity C has outstanding deficiencies dating back to 2013, as of April 2019, it had yet to develop a formal document for prioritizing and tracking the remediation of each of those deficiencies. Rather, Entity C shared with us various PowerPoint presentations it had delivered to its information technology executive committee to give its members an overall update on the status of each finding. However, these presentations do not consistently provide key details such as who is responsible for tracking each deficiency, the strategy for resolving the deficiency, and the target date for completion. Without a process for tracking their status, some of Entity C's deficiencies have remained outstanding for nearly six years. By not implementing timely remediation activities to address known weaknesses in their information security programs, nonreporting entities are failing to fully protect their information assets.

Many Nonreporting Entities Are Not Fully Assessing the Status of Their Information Security

The majority of nonreporting entities we reviewed have not taken steps to develop and document a comprehensive understanding of their information security status. This lack of understanding limits their assurance that they are properly protecting their information assets against unauthorized access, use, disclosure, disruption, modification, or destruction. For example, one of the 10 entities we reviewed has not adopted an information security standard and has never obtained an information security assessment. In addition, five of the 10 have only partially assessed their compliance with their selected information security standards. Although their previous assessments identified information security problems, none of these five entities have a plan or timeline for how they will routinely assess their compliance with the entirety of their standards. Until nonreporting entities ensure that they have achieved compliance with their selected information security standards, weaknesses in their controls may compromise the confidentiality, integrity, and availability of the information systems they use to carry out their day-to-day operations.

Although nonreporting entities are not required to follow the information security and privacy policies, standards, and procedures the technology department prescribes, nine of the 10 nonreporting entities we reviewed asserted that they relied upon various information security standards—which we found to be comparable to the technology department's standards—when developing their information security and privacy policies, plans, and procedures. However, as shown in Table 1, only six of the nonreporting entities had formally adopted the standards. Adopting standards facilitates a more consistent, comparable, and repeatable approach for securing state assets. Moreover, it creates a foundation from which standardized assessment methods and procedures may be used to measure security effectiveness.

We found that formally adopting information security standards correlated with more robust compliance reviews.

We found that formally adopting information security standards correlated with more robust compliance reviews. Specifically, only four of the nonreporting entities we reviewed had fully assessed their compliance, and all four had formally adopted their selected information security standards. Accordingly, we conclude that adopting standards and performing comprehensive security assessments is a best practice for measuring the effectiveness of an information security program. In contrast, Entity D has neither adopted an information security standard nor performed any formal assessment of its information security status. Rather, it relies solely upon the professional judgment of its information technology manager to ensure the security of its information. Without an information security standard or comprehensive assessment of the standards, entities cannot ensure that they are effectively

managing risk; providing for the protection of information assets; and preventing illegal activity, fraud, waste, and abuse in the use of their information assets.

Regardless of whether they have formally adopted information security standards, nine of the 10 nonreporting entities we reviewed indicated that they had performed a self-assessment or contracted with an independent entity to at least partially assess their compliance with their selected standards, as shown in Table 1. However, five of these assessments were limited in scope, and thus there may be additional existing weaknesses that nonreporting entities have yet to identify.

Table 1
Nonreporting Entities' Information Security Standards and Processes

ENTITY	WHICH STANDARD DID THE ENTITY USE TO DEVELOP ITS INFORMATION SECURITY POLICIES AND PROCEDURES?	DID THE ENTITY FORMALLY ADOPT ITS SELECTED STANDARDS?	HOW MUCH OF ITS SELECTED STANDARD HAS THIS ENTITY ASSESSED IN THE LAST THREE YEARS?
A	SAM 5300	X	▲
B	NIST 800-53 and SAM 5300	X	▲*
C	NIST 800-53 and SAM 5300	X	▲
D	No standard selected	X	X
E	ISO/IEC 27000 family	✓	✓
F	NIST 800-53 and SAM 5300	✓	▲
G	NIST 800-53 and SAM 5300	✓	▲
H	ISO/IEC 27000 family	✓	✓
I	ISO/IEC 27000 family	✓	✓
J	ISO/IEC 27000 family, NIST 800-53, and SAM 5300	✓	✓

Source: Analysis of survey responses and documents obtained from the entities above.

✓ = YES / ALL
X = NO / NONE
▲ = PARTIAL

* In response to our audit, Entity B decided to evaluate its compliance with the remaining requirements that its military department assessment did not cover.

Four of the 10 nonreporting entities we reviewed opted to participate in independent security assessments through the military department. As we mention in the Introduction, state law permits the military

department to perform these independent security assessments, which provide a technical evaluation of a state entity's network and selected web applications to identify security vulnerabilities and provide concrete, implementable actions to reduce the possibility of damaging security breaches. The independent security assessments use a limited set of technical controls based on NIST 800-53 and SAM 5300, as selected by the technology department. Consequently, the military department assessment is not designed to evaluate the entity against the entirety of the information security standards it has selected. For example, the military department's assessment criteria do not address the control area of technology recovery. As discussed in Figure 2, technology recovery is the process of creating detailed plans for recovering critical information systems from unanticipated interruptions or disasters. Therefore, the military department assessment may not detect all of the weaknesses that exist in an entity's information security program.

During its review of the four nonreporting entities, the military department identified overall compliance scores ranging from a low of 47 percent to a high of 66 percent for the select requirements it evaluated. The military department also assessed the effectiveness of one entity's program for applying software security updates and concluded that its system security weaknesses were at extreme risk of known exploitation. Although these assessments demonstrate that there is room for improvement, there may be additional areas of noncompliance because the military department assessments look at only a portion of the required standards. For example, for three of the nonreporting entities we reviewed, the military department assessment is the only security assessment they have completed. Consequently, these three entities may have additional information security weaknesses of which they are currently unaware.

The six nonreporting entities that did not fully assess their security controls have not adequately planned for future assessments.

The four nonreporting entities that assessed all of their selected standards generally expect to receive security assessments every two to three years, while the six nonreporting entities that did not fully assess their security controls have not adequately planned for future assessments. For example, they do not have a written plan that specifies how they will fully assess their compliance with the requirements, such as who will perform the assessment, which requirements will be included in each assessment, and how frequently each requirement will be assessed. In July 2018, the military department performed an assessment of Entity B, which resulted in an overall compliance score of 59 percent and 13 findings of deficiency. We followed up with Entity B to see whether it had assessed its compliance with any of the information security controls that were not included in the military department assessment, and Entity B replied that it had not done so. However, in response to our audit, it decided to perform an internal assessment of the remaining controls and concluded that it was

only 51 percent compliant with those controls. In the absence of robust compliance assessments, nonreporting entities lack assurance that their information security controls are implemented correctly, are operating as intended, and are meeting the security requirements.

Most Nonreporting Entities We Reviewed Lack an External Oversight Framework

The nonreporting entities we reviewed were typically responsible for establishing their own information security programs. As we discuss in the Introduction, state law does not apply the technology department's policies and procedures for information security to nonreporting entities. Specifically, state law requires reporting entities to comply with SAM 5300, which in turn requires them to obtain various assessments and to annually certify compliance with SAM 5300. However, nonreporting entities are not subject to these requirements. Nevertheless, Entity D could not demonstrate that it had ever performed a formal assessment of its information security status. Entity D asserted that it had adopted IT security policies, procedures, and methods consistent with generally accepted industry standards. However, it has not developed information security policies or procedures that can guide its information technology department on how to configure or assess its information systems. In addition, we noted that Entity B did not fully assess its selected information security standards until after we started our audit, which resulted in it identifying additional risks. Without assessing their compliance with security standards, nonreporting entities are likely unaware of the full extent of their information security weaknesses.

Most of the nonreporting entities we reviewed asserted that they did not have an external oversight framework that would require them to assess their information security regularly.

Most of the nonreporting entities we reviewed asserted that they did not have an external oversight framework that would require them to assess their information security regularly. However, we noted that those few nonreporting entities that were subject to such a requirement typically assessed more of their selected information security standards than those that had no such requirement. Specifically, three of the four reviewed entities that fully assessed their selected standards were also subject to an oversight framework that required them to assess their information security regularly. We also noted that some nonreporting entities with requirements to perform assessments generally established processes for following up on past findings. For example, Entity E is required to regularly obtain a comprehensive, external security assessment. We found that Entity E's information security assessments covered the entirety of its selected standards, and it asserts that it has resolved all of the issues identified by those assessments. In contrast, Entity A asserted that it does not have external oversight, and it has yet to fully resolve the top five areas of concern that the military

department identified in 2017. Without the accountability that external oversight provides, nonreporting entities may be less likely to resolve information security issues in a timely manner.

These examples demonstrate the value of establishing an oversight framework for nonreporting entities. However, several nonreporting entities have previously expressed concern that reporting to the technology department would jeopardize their independence; therefore, the Legislature may be better positioned to oversee nonreporting entities. It could amend state law to provide a confidential mechanism for these entities to share highly sensitive information about their information security status.

Recommendations

To strengthen the information security practices of nonreporting entities, the Legislature should amend state law to do the following:

- Require all nonreporting entities to adopt information security standards comparable to SAM 5300.
- Require all nonreporting entities to obtain or perform comprehensive information security assessments no less frequently than every three years to determine compliance with the entirety of their adopted information security standards.
- Require all nonreporting entities to confidentially submit certifications of their compliance with their adopted standards to the Assembly Privacy and Consumer Protection Committee and, if applicable, to confidentially submit corrective action plans to address any outstanding deficiencies.

We conducted this audit under the authority vested in the California State Auditor by Government Code 8543 et seq. and according to 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 specified in the Scope and Methodology section of the report. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Respectfully submitted,

ELAINE M. HOWLE, CPA
California State Auditor

Date: July 16, 2019

Appendix

Scope and Methodology

State law authorizes the State Auditor to establish a program to audit and issue reports with recommendations to improve any state agency or statewide issue that the State Auditor identifies as being at high risk for the potential of waste, fraud, abuse, and mismanagement or that has major challenges associated with its economy, efficiency, or effectiveness. In January 2018, we issued our latest assessment of high-risk issues that the State and selected agencies face. Because we continue to include information security as a high-risk issue for the State, we performed this audit of nonreporting entities' information security practices. The table below lists the objectives we developed and the methods we used to address them.

	AUDIT OBJECTIVE	METHOD
1	Review and evaluate the laws, rules, and regulations significant to the audit objectives.	Reviewed relevant laws, rules, regulations, and other background materials.
2	Conduct a survey of state entities that may not be under the authority of the technology department.	• Used the roster of state agencies, departments, boards, constitutional offices and other entities maintained by the Secretary of State's Office to develop a list of 233 potential survey recipients. • Removed various entities from our list, including those that were clearly under the authority of the Governor and entities that had responded to our previous information security survey for reporting entities. • Surveyed the remaining entities to determine whether they are subject to the technology department's authority, and relied upon their responses for categorizing them as either reporting or nonreporting entities. • Using these categorizations, summarized the information security practices of the nonreporting entities we surveyed.
3	For surveyed state entities asserting they are under the authority of the technology department, verify they submitted an information security self-assessment to the technology department.	Obtained documentation from the technology department and verified that each entity submitted the required information.

continued on next page . . .

	AUDIT OBJECTIVE	METHOD
4	For a selection of state entities that indicated that they are not subject to the authority of the technology department, do the following: a. Review information security standards adopted by nonreporting entities and determine if they are comparable to the standards adopted by the technology department. b. Review nonreporting entities' assessments and determine whether the scope of work performed covers the entirety of their selected standards.	• Selected 10 nonreporting entities based on various factors from their survey responses, such as the standards they specified, whether they had an independent security assessment, and the time since their most recent assessment, among others. • Interviewed staff at each of the selected entities to gain an understanding of its information security practices. • Reviewed the information security standards of the selected nonreporting entities and compared their control areas to those found within SAM 5300. We determined that the selected standards were comparable. • Obtained and reviewed information security assessments and other documentation from selected entities. Using these documents, we determined whether the information security assessments reviewed each of the key control areas of the nonreporting entities' selected standards. However, we did not determine if nonreporting entities assessed each control within each control area. In addition, we followed up on select high-risk findings identified by the information security assessments to determine whether the nonreporting entity had a process for resolving them.
5	Review and assess any other issues that are significant to the audit.	Reviewed the State Leadership Accountability Act (accountability act) reports of our selected nonreporting entities to determine whether they identified information security as a concern. The accountability act requires the Department of Finance to identify state entities that must report biennially to the Legislature on the adequacy of their systems of internal control—which may include information security. Entities are allowed to choose the number and types of risks to include in their reports, which must be made public. Only three of the 10 nonreporting entities we reviewed used these reports to communicate information security issues. In addition, because accountability act reports are public documents, entities would only be able to share limited information about their information security issues without compromising their systems. As a result, we determined that accountability act reports were not specifically designed to provide external oversight of a nonreporting entity's information security posture.

Source: Analysis of information and documentation identified in the column titled Method.