State High-Risk Update— Information Security

The California Department of Technology's Inadequate Oversight Limits the State's Ability to Ensure Information Security

January 2022

REPORT 2021-602

```
ction == "MIRROR_Z":
_mod.use_x = False
_mod.use_y = False
_mod.use_z = True

ction at the end -add back the desele
b.select= 1
_ob.select=1
t.scene.objects.active = modifier_ob
lected" + str(modifier_ob)) # modifie
_ob.select = 0
.context.selected_objects[0]
.objects[one.name].select = 1
("please select exactly two objects,
OPERATOR CLASSES ----------------
```

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 our Public Affairs Office at 916.445.0255
This report is also available online at www.auditor.ca.gov | Alternative format reports available upon request | Permission is granted to reproduce reports

Michael S. Tilden *Acting State Auditor*

January 18, 2022
2021-602

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

Dear Governor and Legislative Leaders:

As authorized by state law, my office conducted a state high-risk audit of the State's information security. Our assessment focused on the California Department of Technology's (CDT) oversight of information security for state entities within the executive branch that are under the Governor's direct authority (reporting entities). For entities that fall outside of CDT's purview (nonreporting entities), we evaluated their compliance with their selected security standards. The following report details our conclusion that the State's approach to oversight has limited its progress toward ensuring the security of its information.

We found that CDT has yet to establish an overall statewide information security status for the State's 108 reporting entities. CDT relies on compliance audits and technical security assessments to summarize each reporting entity's information security development into a single score, called a *maturity metric*. However, because CDT was slow to complete compliance audits, it only calculated 18 of the 39 maturity metric scores it should have determined by June 2021. Despite being aware of shortcomings with its approach, CDT failed to expand its capacity to perform compliance audits.

Moreover, even though CDT requires reporting entities to complete various self-assessments of their information security each year, it does not use this information to inform the statewide security status. Nonetheless, the information CDT does have shows that reporting entities continue to perform below recommended standards, and have not improved over the last several years. However, CDT has not taken critical steps to help reporting entities improve, such as holding them accountable for identifying potential risks to their critical information systems.

Finally, we surveyed 32 nonreporting entities and found that they also have not adequately addressed their information security. Although 29 of the 32 nonreporting entities have adopted an information security framework or standards, only four reported that they achieved full compliance with their chosen framework or standards. We previously noted that some nonreporting entities have an external oversight framework that requires them to assess their information security regularly. In fact, we found that nonreporting entities with external oversight were generally further along in their information security development. Accordingly, we recommended that the Legislature create an oversight structure for all nonreporting entities.

Respectfully submitted,

MICHAEL S. TILDEN, CPA
Acting California State Auditor

Selected Abbreviations Used in This Report

CDT	California Department of Technology
IT	information technology
maturity metric	California Cybersecurity Maturity Metric
Military Department	California Military Department
nationwide review	Nationwide Cybersecurity Review
NIST 800-53	*National Institute of Standards and Technology Special Publication 800-53*
nonreporting entities	entities that fall outside of the Governor's direct authority
reporting entities	state entities within the executive branch that are under the Governor's direct authority
SAM	*State Administrative Manual*
SIMM	*Statewide Information Management Manual*

Contents

Blank page inserted for reproduction purposes only.

SUMMARY

Results in Brief

Information security measures are critical to safeguarding the State's data processing capabilities, information technology (IT) infrastructure, and data, all of which are essential public resources. Without adequate information security, cyberattacks such as phishing and malware intrusions can result in the disclosure of confidential information or the shutdown of critical information systems. The California Department of Technology (CDT) is responsible for providing policies and procedures 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 policies and procedures that CDT prescribes and to regularly report to CDT on their compliance. State law does not apply CDT's requirements to entities that fall outside of the Governor's direct authority (nonreporting entities).

Although one of CDT's key roles is to oversee information security development for the State's 108 reporting entities, it has yet to fully assess the overall status of the State's information security. In fiscal year 2018–19, CDT implemented a four-year oversight life cycle to independently verify the information security status of 52 high-risk reporting entities. This oversight life cycle calls for CDT to use compliance audits and technical security assessments to summarize each reporting entity's information security development level into a single score, which it refers to as a *maturity metric*. However, because CDT has been slow to complete the compliance audits, it had calculated only 18 of the 39 maturity metric scores it should have determined by the conclusion of the third year of the oversight life cycle in June 2021. Despite being aware of shortcomings with its approach, CDT has failed to take proactive steps to expand its capacity to perform the compliance audits, such as hiring more auditors or repurposing existing staff. Moreover, even though CDT requires reporting entities to complete self-assessments of their information security development each year, it has not used this information to inform the overall status of the State's information security.

In fact, when we evaluated reporting entities' maturity metrics and self-reported information, we found that many entities' information security is below standards. We also found little to suggest improvement over the last several years. Moreover, because CDT generally provides information on only certain aspects of the State's information security in its reports to the Legislature, the Legislature does not have a complete picture of the deficiencies in the reporting entities' information security statuses.

Audit Highlights . . .

Our audit of the information security practices of state entities that report to the Governor (reporting entities) and state entities that fall outside of the Governor's direct authority (nonreporting entities) found the following:

- *CDT has been slow to assess the information security status of reporting entities and has failed to proactively expand its capacity to do so.*
- *CDT has not held reporting entities accountable for performing required self-assessments.*
- *CDT does not use the self-reported information it has collected to inform the overall status of the State's information security.*
- *CDT has not updated its security and privacy policies to align with federal standards.*
- *CDT's guidance about information security relative to teleworking policies and training is not entirely clear.*
- *Many reporting entities' information security is below standards and has not improved over the last several years.*
- *Among nonreporting entities, few are fully compliant with their chosen information security standards and some have not yet even adopted such a standard or framework.*
- *The Legislature should create an oversight structure for nonreporting entities to better hold them accountable for improving their information security.*

The reporting entities' lack of progress in developing their own information security may be in part because CDT has failed to take critical steps to help them improve. For example, it did not adequately follow up with 18 of the 108 reporting entities whose directors have not submitted required certifications indicating that they were fully aware of their entities' information security statuses, were aware of any identified risks, and recognized that all deficiencies had to be addressed. CDT also failed to hold reporting entities accountable for completing the required self-assessments for only 172 of their 3,300 critical IT systems. Consequently, the reporting entities' updates to CDT on their progress toward remediating any known weaknesses are incomplete. Because CDT uses these updates to identify common issues that may exist across the State so that it can provide additional training, it lacks assurance that it is focusing its oversight efforts on the areas at highest risk to the State. Further, because CDT did not promptly revise the State's information security and privacy policies to align with federal standards that went into effect more than a year ago, the State's policies have continued to direct reporting entities to an outdated version of federal information security standards with which they are required to comply.

A specific area of concern that has recently emerged for the State is the potential increase in security risks posed by widespread telework resulting from the COVID-19 pandemic. At the start of the pandemic, CDT took emergency steps to assist reporting entities as they prepared for an increase in teleworking, and the five reporting entities we reviewed generally had appropriate telework policies and trainings. However, the guidance CDT provided for securing a personal device for telework was unclear because it implied that some steps were only required in limited circumstances. By clarifying the guidance, CDT can help reporting entities ensure that employees using a personal device to telework have taken all of the required measures to secure their devices.

Finally, when we surveyed 32 nonreporting entities, we found that they also have not adequately addressed their information security. Although 29 of the 32 nonreporting entities have adopted an information security framework or standards, only four reported that they had achieved full compliance with their chosen framework or standards. In addition, of the 20 surveyed nonreporting entities that allow employees to use personally owned devices for teleworking, only five provided any training on properly configuring and securing personal devices. In our previous report, we identified gaps in oversight that have contributed to nonreporting entities' information security weaknesses.[1] We also noted that some nonreporting entities

[1] *High Risk Update—Information Security: Gaps in Oversight Contribute to Weaknesses in the State's Information Security,* Report 2018-611, July 2019.

have an external oversight framework that requires them to assess their information security regularly. We found that nonreporting entities with external oversight were generally further along in their information security development than those without such oversight. Given the value of external oversight of information security and considering our recent survey results, the Legislature should create an oversight structure for all nonreporting entities.

Selected Recommendations

Legislature

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

- Require that CDT confidentially submit an annual statewide information security status report, including maturity metric scores and self-reported information, to the appropriate legislative committees no later than December 2022. This status report should include CDT's plan for assisting reporting entities in improving their information security.
- Require each nonreporting entity to adopt information security standards comparable to those required by CDT and to provide a confidential, annual status update on its compliance with its adopted information security standards to legislative leadership, including the president pro tempore of the California State Senate, the speaker of the California State Assembly, and minority leaders in both houses. It should also require each nonreporting entity to perform or obtain an audit of its information security no less frequently than every three years.
- Require nonreporting entities that allow employees to telework to develop telework policies and training comparable to those CDT requires.

CDT

To ensure that it understands the statewide security status of reporting entities, CDT should do the following:

- Increase its capacity to perform timely compliance audits—which may entail hiring more staff or securing additional contracted audit support—by the conclusion of the four-year oversight life cycle in June 2022.

- Until it is able to conduct timely, objective audits of reporting entities, CDT should follow up with reporting entities annually to ensure that they complete the required self-assessments of their critical IT systems.

- Utilize the information from the various self-assessments the reporting entities complete annually to help identify common areas that require improvement across multiple reporting entities.

To help ensure that reporting entities are aware of new federal information security standards that are intended to strengthen their security and privacy governance, CDT should complete the necessary updates to the State's information security and privacy policies by June 2022.

To help reporting entities ensure that their teleworking employees are taking appropriate security precautions, CDT should clarify guidance by February 2022 to require all employees using personal devices for state business to implement baseline security measures.

Agency Comments

Although CDT stated it appreciated us providing valuable insights related to its oversight, it disagreed with many of the conclusions of the report. Further, CDT generally did not address our recommendations in its response.

INTRODUCTION

Background

Information security incidents that compromised the integrity, confidentiality, or availability of information have affected numerous retailers, government agencies, and financial institutions in recent years. Some of these security breaches have resulted in the disclosure of confidential information or the shutdown of information systems and critical infrastructure. For example, in June 2020, individuals launched a ransomware attack that encrypted the data on a number of servers at the University of California, San Francisco (UCSF) School of Medicine. To recover the data, UCSF paid approximately $1.1 million to the individuals behind the attack. In another example, in March 2021, an employee at the State Controller's Office (SCO) clicked on a link in an email that appeared to come from a trusted outside entity and unknowingly provided a hacker with access to reports that may have included individuals' full names, addresses, Social Security numbers, and birth dates. The hacker then sent malicious emails to the employee's contacts.

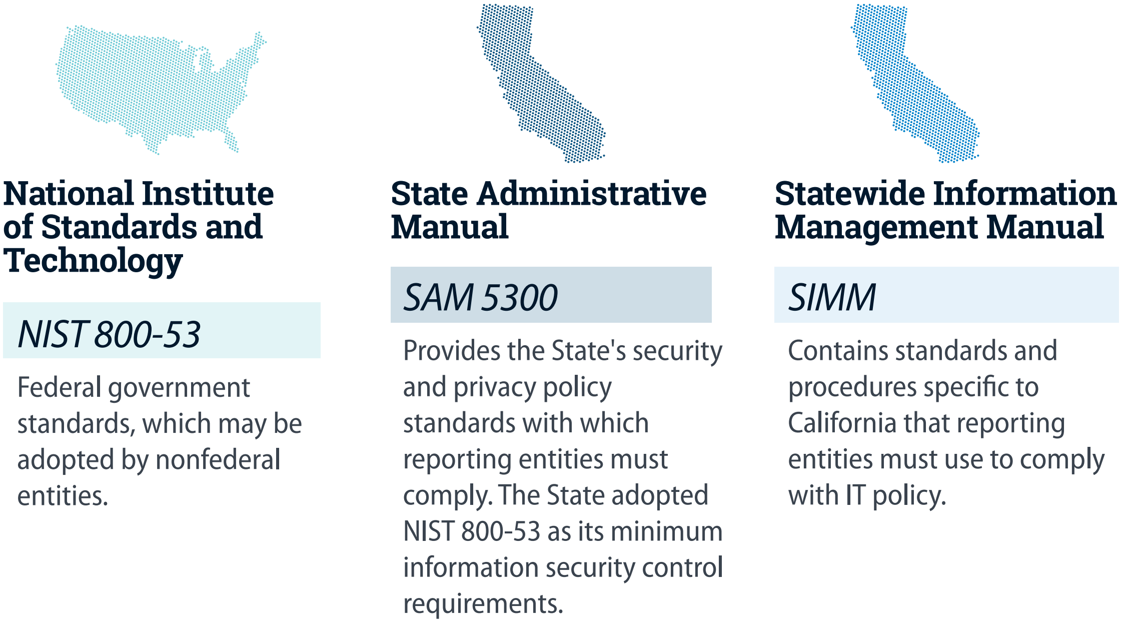
These incidents demonstrate the importance of information security. *Information security* refers to protection of information assets, such as the servers compromised at UCSF and the email and data compromised at the SCO. The State's information assets—including its data processing capabilities, information technology (IT) infrastructure, and data—are an essential public resource. In fact, many state entities would need to effectively cease their program operations in the absence of key computer systems. Implementing appropriate security measures and controls is critical to ensuring the confidentiality, integrity, and availability of the information and systems.

The California Department of Technology (CDT) is responsible for providing direction for the State's information security. State law generally requires state agencies within the executive branch that are under the Governor's direct authority (reporting entities) to comply with the information security policies and procedures that CDT prescribes and to regularly report to CDT on their compliance. In addition, information security falls within the scope of three legislative committees. These include the Senate Select Committee on Cybersecurity and Identity Theft Prevention, the Assembly Select Committee on Cybersecurity, and the Assembly Standing Committee on Privacy and Consumer Protection, which is responsible for oversight of CDT. CDT's policies and procedures do not apply to entities that fall outside of the Governor's direct authority (nonreporting entities), such as constitutional offices and judicial branch courts and agencies. The State does not mandate oversight of information security for all nonreporting entities.

Information Security Standards for Reporting Entities

State law requires CDT to issue and maintain policies, standards, and procedures governing information security for reporting entities. In response, CDT developed Chapter 5300 of the *State Administrative Manual* (SAM 5300), which provides the security and privacy policy standards with which reporting entities must comply. SAM 5300 also 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. Further, as Figure 1 shows, CDT provides additional information security standards and procedures that reporting entities must comply with in its *Statewide Information Management Manual* (SIMM).

Figure 1
Reporting Entities Must Comply With Three Information Security Standards



National Institute of Standards and Technology

NIST 800-53

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

State Administrative Manual

SAM 5300

Provides the State's security and privacy policy standards with which reporting entities must comply. The State adopted NIST 800-53 as its minimum information security control requirements.

Statewide Information Management Manual

SIMM

Contains standards and procedures specific to California that reporting entities must use to comply with IT policy.

Source: NIST 800-53, SAM 5300, and SIMM.

CDT's Oversight of Reporting Entities

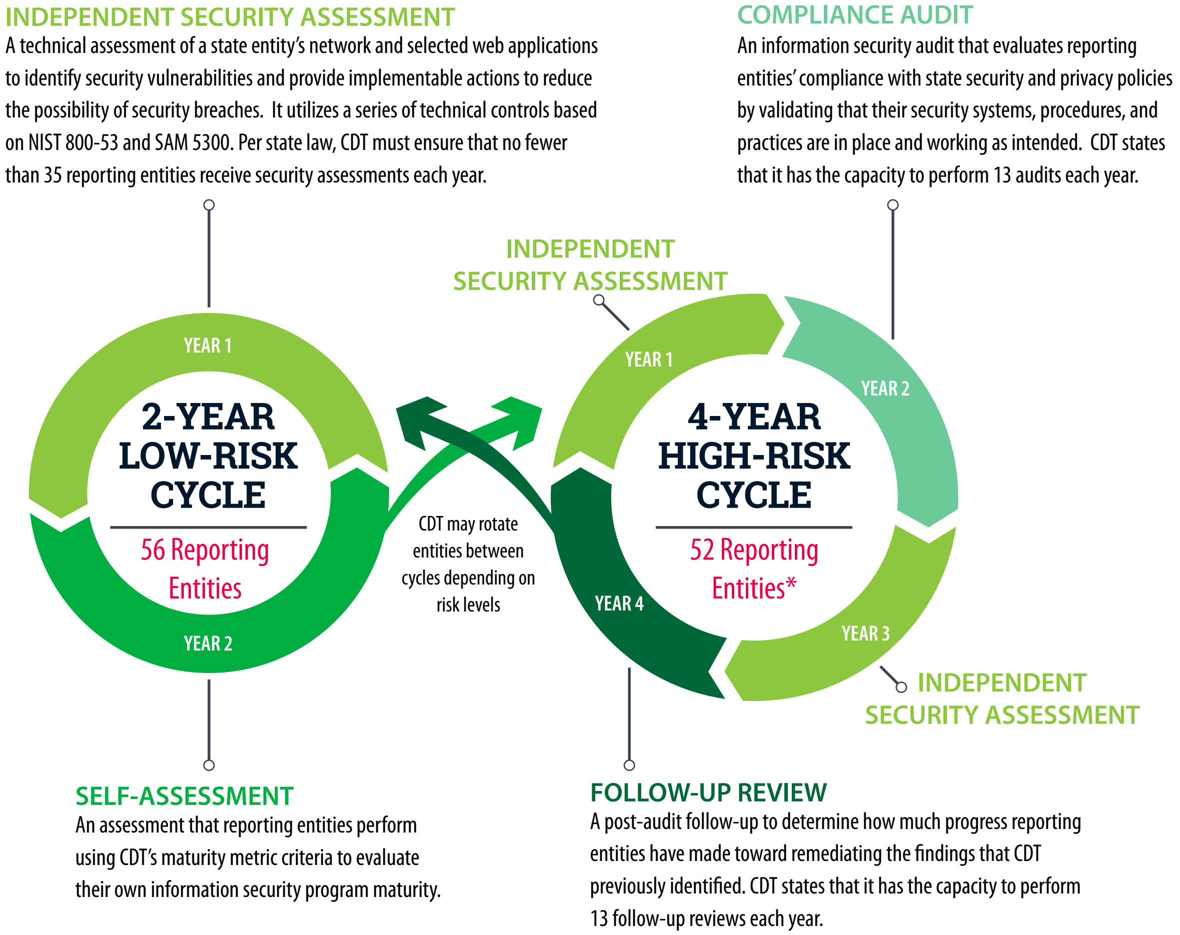
Although reporting entities are ultimately responsible for their own information security, CDT plays a critical role in advising them on security issues and helping to ensure their compliance with state policy. In fiscal year 2018–19, CDT implemented a four-year oversight life cycle to independently verify the status of the State's information security. As Figure 2 shows, the four-year oversight life cycle consists of both an initial compliance audit and a follow-up review, in addition to two independent security assessments. Using a risk-based methodology, CDT prioritized 52 high-risk entities to participate in the first four-year cycle.[2] CDT's risk analysis considered various factors, such as the type of data that entities store, the nature of their business, the maturity of their overall information security programs, and their likelihood of facing threats that necessitate a high level of attention and monitoring.

CDT requires the remaining, lower-risk reporting entities to participate in a two-year oversight life cycle. In this two-year cycle, they receive one independent security assessment and are responsible for performing a self-assessment of their own information security development. As entities' information security statuses evolve and risks change, CDT may rotate entities between the four-year and two-year oversight life cycles.

According to the state chief information security officer (state chief), CDT has the capacity to complete 13 compliance audits and 13 follow-up reviews each year. CDT conducts audits and follow-up reviews to evaluate entities' compliance with the State's information security and privacy policies by validating that their security systems, policies, procedures, and practices are in place and working as intended. Each audit—which is based on SAM 5300 and NIST 800-53—culminates in a report that highlights CDT's findings and observations and in a post-audit workshop where CDT assists the entity in planning its approach to remediating identified findings. The follow-up review is a more narrowly scoped evaluation, focusing on the progress the entity has made addressing the previously identified findings. The follow-up review also culminates with an audit report and a post-audit workshop.

[2] CDT invited some nonreporting entities to participate in the four-year cycle.

Figure 2
CDT Performs More Extensive Information Security Oversight for High-Risk Reporting Entities



INDEPENDENT SECURITY ASSESSMENT
A technical assessment of a state entity's network and selected web applications to identify security vulnerabilities and provide implementable actions to reduce the possibility of security breaches. It utilizes a series of technical controls based on NIST 800-53 and SAM 5300. Per state law, CDT must ensure that no fewer than 35 reporting entities receive security assessments each year.

COMPLIANCE AUDIT
An information security audit that evaluates reporting entities' compliance with state security and privacy policies by validating that their security systems, procedures, and practices are in place and working as intended. CDT states that it has the capacity to perform 13 audits each year.

SELF-ASSESSMENT
An assessment that reporting entities perform using CDT's maturity metric criteria to evaluate their own information security program maturity.

FOLLOW-UP REVIEW
A post-audit follow-up to determine how much progress reporting entities have made toward remediating the findings that CDT previously identified. CDT states that it has the capacity to perform 13 follow-up reviews each year.

YEAR 1
2-YEAR LOW-RISK CYCLE
56 Reporting Entities
YEAR 2
CDT may rotate entities between cycles depending on risk levels
INDEPENDENT SECURITY ASSESSMENT
YEAR 1
YEAR 2
4-YEAR HIGH-RISK CYCLE
52 Reporting Entities*
YEAR 4
YEAR 3
INDEPENDENT SECURITY ASSESSMENT

Source: Interviews with CDT staff and review of documents.

Note: Entities will not receive an audit or follow-up review during the same year that they receive an independent security assessment.

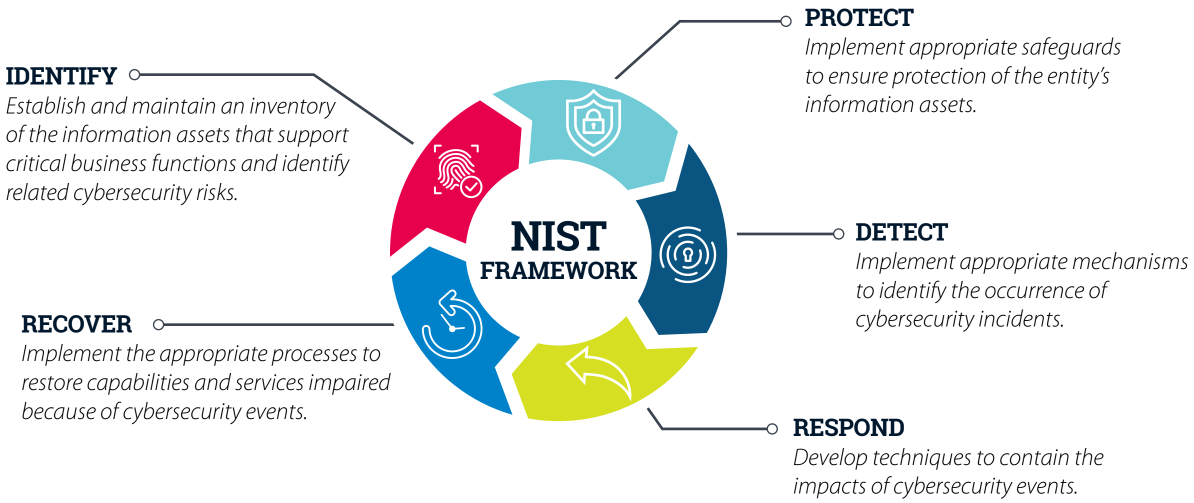
* CDT invited some nonreporting entities to participate in the four-year high-risk cycle.

Whereas CDT designed the compliance audits to assess an entity's adherence to the State's information security and privacy policies, the independent security assessments evaluate the actual implementation, configuration, and practices of the entity's information security program. State law requires CDT to either conduct or require another entity to conduct no fewer than 35 independent security assessments of reporting entities each year. CDT currently contracts with the California Military Department (Military Department) to perform the independent security assessments, although reporting entities may request permission from CDT to use a third-party vendor.

California Cybersecurity Maturity Metrics

CDT established the California Cybersecurity Maturity Metrics (maturity metrics) to combine the results of its compliance audits and the Military Department's independent security assessments into a single score for each reporting entity that summarizes that entity's information security development. The maturity metrics measure an entity's performance on five information security functions, as Figure 3 shows. According to the state chief, the four-year oversight life cycle should culminate in a maturity metric score for each of the 52 high-risk entities that CDT evaluates. Consequently, CDT cannot calculate a maturity metric score for an entity until both the entity's compliance audit and its independent security assessments are complete.

Figure 3
CDT's Maturity Metrics Measure Entities' Performance on Five Core Information Security Functions



PROTECT
Implement appropriate safeguards to ensure protection of the entity's information assets.

IDENTIFY
Establish and maintain an inventory of the information assets that support critical business functions and identify related cybersecurity risks.

DETECT
Implement appropriate mechanisms to identify the occurrence of cybersecurity incidents.

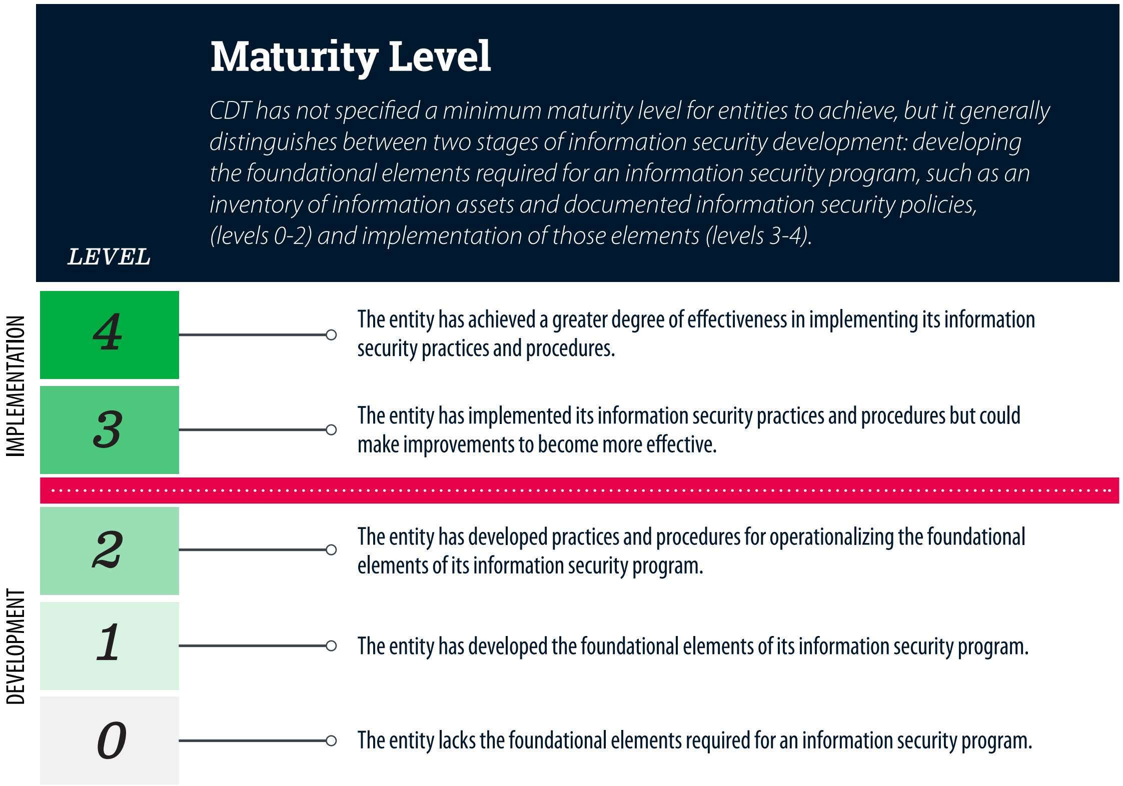
RECOVER
Implement the appropriate processes to restore capabilities and services impaired because of cybersecurity events.

RESPOND
Develop techniques to contain the impacts of cybersecurity events.

Source: NIST Cybersecurity Framework website.

As Figure 4 shows, the maturity metrics utilize a scale of 0 to 4. Although CDT has not identified a minimum recommended score for entities to achieve, it distinguishes between two levels of information security development. Specifically, entities that score a value between 0 and 2 are still working to develop the foundational components of their information security program or have developed them, whereas entities that score a value of 3 or 4 have already implemented their procedures and have demonstrated varying levels of effectiveness. CDT designed the maturity metrics to be repeatable and consistent so that it can gauge each entity's progress moving forward and compare information security development across entities. For those reasons, the statewide cybersecurity metrics program manager (metrics manager) explained that CDT does not intend to change the methodology for calculating maturity metric scores during the four-year oversight life cycle. In addition to using the maturity metrics to identify gaps in a specific entity's information security, CDT uses the maturity metrics to track statewide trends that can inform the control categories for which it offers additional guidance, training, and support.

Figure 4
Higher Scores on the Maturity Metrics Reflect Higher Information Security Maturity Levels



Maturity Level

CDT has not specified a minimum maturity level for entities to achieve, but it generally distinguishes between two stages of information security development: developing the foundational elements required for an information security program, such as an inventory of information assets and documented information security policies, (levels 0-2) and implementation of those elements (levels 3-4).

LEVEL

IMPLEMENTATION

4 — The entity has achieved a greater degree of effectiveness in implementing its information security practices and procedures.

3 — The entity has implemented its information security practices and procedures but could make improvements to become more effective.

DEVELOPMENT

2 — The entity has developed practices and procedures for operationalizing the foundational elements of its information security program.

1 — The entity has developed the foundational elements of its information security program.

0 — The entity lacks the foundational elements required for an information security program.

Source: Interviews with CDT staff and review of CDT's maturity metrics.

Reporting Entities' Self-Reporting Mechanisms

CDT requires reporting entities to participate in several self-reporting mechanisms related to their information security, as summarized in the text box. For example, CDT requires reporting entities to complete the federal Nationwide Cybersecurity Review (nationwide review) every year because it is a condition for receiving information security grant funding from the U.S. Department of Homeland Security. The nationwide review is a self-assessment questionnaire that reporting entities submit to the federal government. It allows entities to rate on a scale of 1 to 7 how well they are addressing different information security activities within NIST, thus providing an entitywide information security assessment. As Figure 5 shows, higher scores on the nationwide review are indicative of more advanced information security development. The minimum recommended maturity level on the nationwide review is a score of 5. Upon completion of the nationwide review, entities have access to custom individual reports.

In addition, CDT also requires reporting entities to perform a security controls self-assessment based on NIST 800-53 for each of their critical IT systems to identify security risks related to that system and establish a plan to resolve those risks. CDT's user guide for the self-assessment explains that by proactively reviewing their information systems, entities can help prevent security breaches and thus protect the valuable information entrusted to the State. Further, the security controls self-assessments can also aid reporting entities in determining their information security budgets, priorities, and resources. CDT directs reporting entities with several critical IT systems to assess the most critical first.

The security controls self-assessment culminates with a high-risk findings report, which entities must submit to CDT as part of their annual Information Security and Privacy Program Compliance Certifications (compliance certifications). In this document, a reporting entity's director, or equivalent head, certifies that he or she has been fully briefed on the entity's information security status, is aware of any identified risks, and recognizes that all deficiencies must be addressed to ensure compliance with the State's information security and privacy requirements. The state chief explained that the compliance certification allows CDT to hold each entity's director accountable for its information security.

Descriptions of Reporting Entities' Self-Reporting Mechanisms

Nationwide Review

- Self-assessment questionnaire that entities complete each year and submit directly to the federal government.
- Provides an overall, entitywide assessment of their information security status.
- Required by CDT because it is a condition for receiving information security grants from the federal government.

Security Controls Self-Assessment

- Self-assessment that reporting entities perform to evaluate each of their critical IT systems for potential security risks and establish plans to resolve them.
- Culminates with a high-risk findings report, which entities must submit to CDT.
- Helps to proactively prevent security breaches and protect the valuable information entrusted to the State.

Compliance Certification

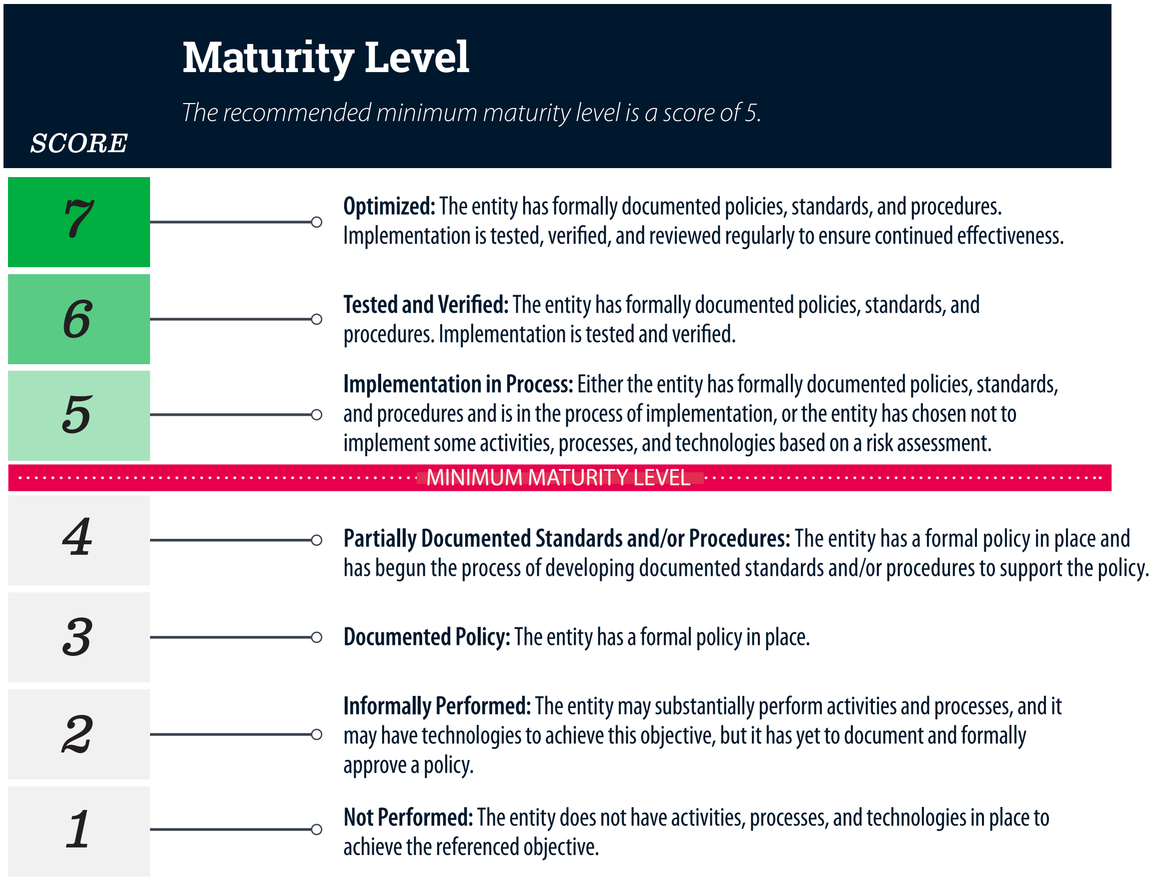
- Document that the director, or equivalent head of the entity, submits to CDT each year acknowledging his or her responsibility for the entity's risk management.
- Holds the head of the entity accountable for the entity's information security status.

Plan of Action

- Document that entities develop, maintain, and utilize to provide at least quarterly updates to CDT on their progress toward remediating any known information security weaknesses.
- CDT compiles the plans of action across all entities to identify the top NIST control categories for which the State has outstanding issues. This helps identify specific areas where entities may need additional training.

Source: Interviews with CDT staff and review of documents.

Figure 5
Higher Scores on the Nationwide Review Reflect Higher Information Security Maturity Levels



Maturity Level

The recommended minimum maturity level is a score of 5.

SCORE

7 — **Optimized:** The entity has formally documented policies, standards, and procedures. Implementation is tested, verified, and reviewed regularly to ensure continued effectiveness.

6 — **Tested and Verified:** The entity has formally documented policies, standards, and procedures. Implementation is tested and verified.

5 — **Implementation in Process:** Either the entity has formally documented policies, standards, and procedures and is in the process of implementation, or the entity has chosen not to implement some activities, processes, and technologies based on a risk assessment.

MINIMUM MATURITY LEVEL

4 — **Partially Documented Standards and/or Procedures:** The entity has a formal policy in place and has begun the process of developing documented standards and/or procedures to support the policy.

3 — **Documented Policy:** The entity has a formal policy in place.

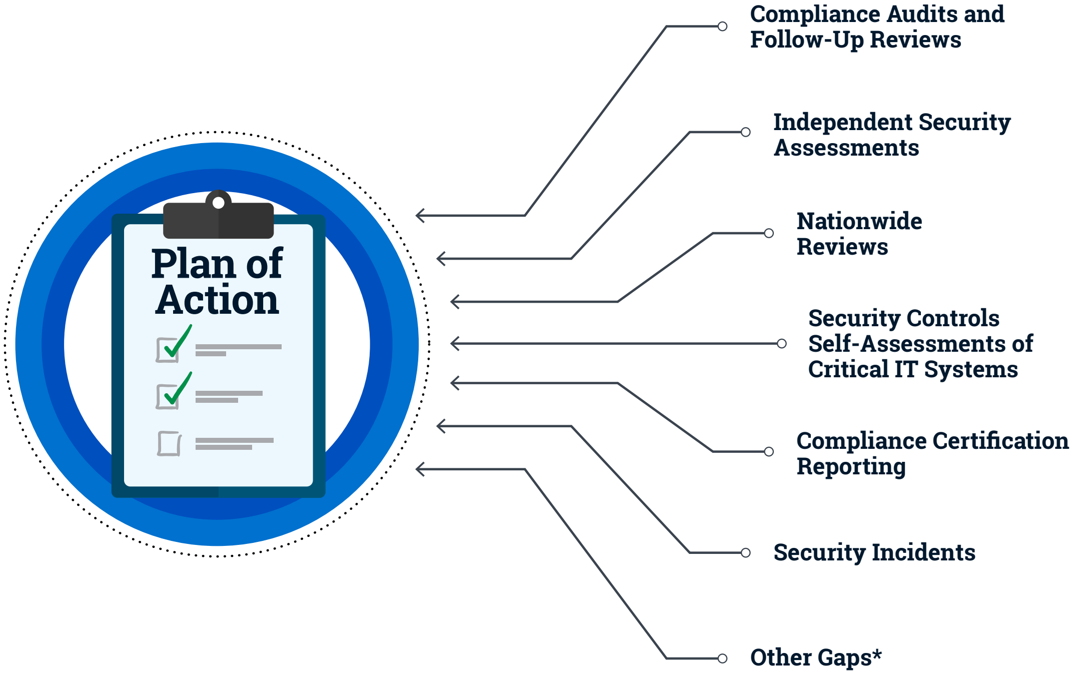
2 — **Informally Performed:** The entity may substantially perform activities and processes, and it may have technologies to achieve this objective, but it has yet to document and formally approve a policy.

1 — **Not Performed:** The entity does not have activities, processes, and technologies in place to achieve the referenced objective.

Source: Nationwide review.

Finally, CDT requires reporting entities to develop and maintain a Plan of Action and Milestones document (plan of action), which they must use to provide, at a minimum, quarterly updates to CDT on their progress toward remediating any known information security weaknesses. As Figure 6 shows, the plan of action is a document that reporting entities regularly update with information security deficiencies identified through the compliance activities we describe previously. CDT expects reporting entities to also track in their plans of action any information security weaknesses that they identify through other sources, such as security incidents or third‑party oversight reviews. For each deficiency in the plan of action, reporting entities must briefly describe the high‑level steps they will take to address the risk and whether they have identified any constraints to remediating the risk, among other things. According to the information security statewide risk management program manager (risk manager), CDT periodically compiles all the entities' plans of action to identify the top NIST control categories in which the State has outstanding issues so that it can provide additional training as needed.

Figure 6
An Entity's Plan of Action Tracks Its Progress Toward Remediating Information Security Deficiencies That Various Sources Have Identified


Plan of Action
Compliance Audits and Follow-Up Reviews
Independent Security Assessments
Nationwide Reviews
Security Controls Self-Assessments of Critical IT Systems
Compliance Certification Reporting
Security Incidents
Other Gaps*

Source: Interviews with CDT staff and review of documents.

* The plan of action should include any significant information security risks that cannot be immediately addressed, regardless of how those risks are identified. Such risks would include a vendor notifying the entity that an information system will no longer be supported or a consulting firm identifying unmitigated vulnerabilities after performing a risk assessment.

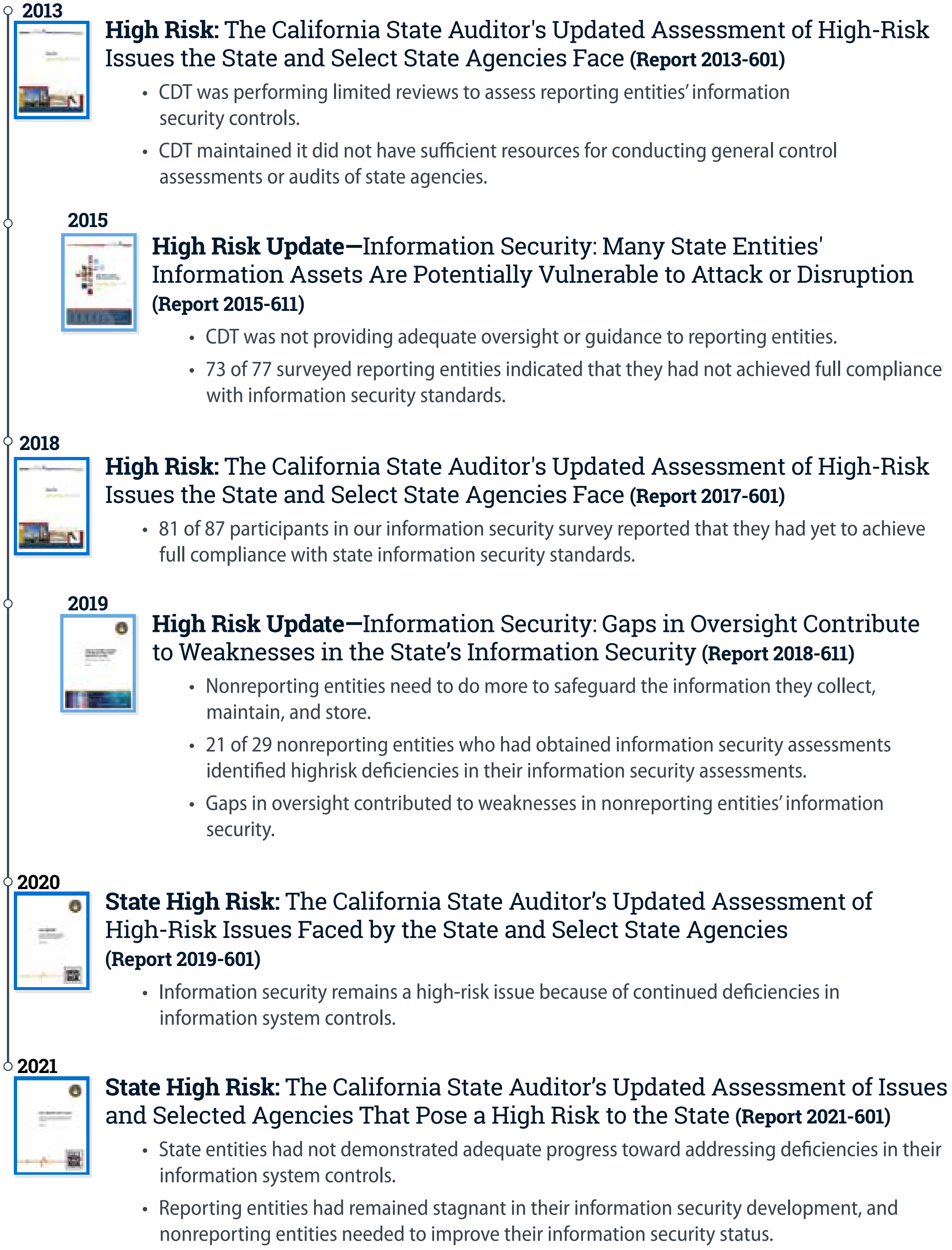
The State's Recent Establishment of Cal-Secure

In addition to the information security oversight measures and programs we describe above, Governor Newsom's administration announced Cal-Secure in October 2021. A multiyear cybersecurity road map, Cal-Secure is designed to address critical gaps in the State's information and cybersecurity programs while enabling the State to manage existing and future threats more effectively. It includes a prioritized list of baseline cybersecurity capabilities that all reporting entities must achieve over the next five years, including an antiphishing program, security and privacy awareness training, and software supply chain management. At the close of each fiscal year, entities will be required to attest that they have achieved the required capabilities, and CDT will provide an update on the implementation status of Cal-Secure initiatives. We did not assess the effectiveness of Cal-Secure because not enough time has passed since it was announced in October 2021 to measure whether it helped strengthen the State's cybersecurity.

Our Identification of Information Security as a High-Risk Issue for Reporting and Nonreporting Entities

State law authorizes the California State Auditor's Office (State Auditor) to develop a program for identifying, auditing, and reporting on high-risk state entities and statewide issues. As Figure 7 shows, we first identified information security as a high-risk issue in 2013 when we concluded that CDT was performing limited reviews to assess the security controls that reporting entities had implemented for their information systems. Since that time, we have issued five reports related to this issue, all of which have identified similar, ongoing deficiencies. CDT plays a role in various activities related to the State's information security, such as performing comprehensive monitoring and detecting advanced cyberthreats through its Security Operations Center and mitigating, identifying, responding to, and reporting information security incidents. However, for the current audit, we focused on CDT's oversight of reporting entities' information security, including their efforts related to telework. We also evaluated nonreporting entities' compliance with their selected security standards, as well as their adoption of best practices related to telework.

Figure 7
We Have Reported on the State's High-Risk Information Security Since 2013



2013

High Risk: The California State Auditor's Updated Assessment of High-Risk Issues the State and Select State Agencies Face **(Report 2013-601)**

- CDT was performing limited reviews to assess reporting entities' information security controls.
- CDT maintained it did not have sufficient resources for conducting general control assessments or audits of state agencies.

2015

High Risk Update—Information Security: Many State Entities' Information Assets Are Potentially Vulnerable to Attack or Disruption **(Report 2015-611)**

- CDT was not providing adequate oversight or guidance to reporting entities.
- 73 of 77 surveyed reporting entities indicated that they had not achieved full compliance with information security standards.

2018

High Risk: The California State Auditor's Updated Assessment of High-Risk Issues the State and Select State Agencies Face **(Report 2017-601)**

- 81 of 87 participants in our information security survey reported that they had yet to achieve full compliance with state information security standards.

2019

High Risk Update—Information Security: Gaps in Oversight Contribute to Weaknesses in the State's Information Security **(Report 2018-611)**

- Nonreporting entities need to do more to safeguard the information they collect, maintain, and store.
- 21 of 29 nonreporting entities who had obtained information security assessments identified highrisk deficiencies in their information security assessments.
- Gaps in oversight contributed to weaknesses in nonreporting entities' information security.

2020

State High Risk: The California State Auditor's Updated Assessment of High-Risk Issues Faced by the State and Select State Agencies **(Report 2019-601)**

- Information security remains a high-risk issue because of continued deficiencies in information system controls.

2021

State High Risk: The California State Auditor's Updated Assessment of Issues and Selected Agencies That Pose a High Risk to the State **(Report 2021-601)**

- State entities had not demonstrated adequate progress toward addressing deficiencies in their information system controls.
- Reporting entities had remained stagnant in their information security development, and nonreporting entities needed to improve their information security status.

Source: State Auditor reports.

Blank page inserted for reproduction purposes only.

AUDIT RESULTS

CDT's Implementation of Its Four-Year Oversight Life Cycle Is Not Sufficient to Assess the Status of the State's Information Security

Although reporting entities are ultimately responsible for their own information security, CDT asserts that for information security programs to improve, it must be able to effectively measure the information security status across the State and within each reporting entity individually. To do this, CDT relies primarily upon its four-year oversight life cycle. As we explain in the Introduction, the four-year oversight life cycle is supposed to culminate in a maturity metric for each of the 52 high-risk entities that CDT evaluates. CDT developed the maturity metrics to combine information from its compliance audits and from the Military Department's independent security assessments. However, CDT has been slow to calculate the maturity metric scores for the entities it audits. Further, it only evaluates reporting entities that it has identified as high risk. Thus, CDT's implementation of its four-year oversight life cycle is not adequate to provide timely, objective maturity metrics of all—or even most—reporting entities. Consequently, CDT does not yet know the status of the State's information security.

CDT is unable to assess all 108 reporting entities during a single four-year period. Rather, before the start of its first oversight life cycle in fiscal year 2018–19, CDT estimated that it had the capacity to evaluate 52 entities during a single four-year cycle. Therefore, it performed a risk assessment to help it prioritize which entities to review first. However, it has been slow to calculate maturity metrics for the 52 entities participating in its first four-year cycle. Specifically, CDT had calculated maturity metric scores for only 17 reporting entities and one nonreporting entity by the conclusion of the third year of the oversight life cycle in June 2021, whereas it should have calculated maturity metric scores for 39 entities in that time frame.

CDT's progress toward establishing the State's information security status has been hampered by its delays in completing its audits.

CDT's progress toward establishing the State's information security status has been hampered by its delays in completing its audits. CDT's intention is to provide compliance audits to all 52 entities during the four-year cycle. However, by the end of the third year, it had completed only 31 of the 39 audits it should have finished. The state chief stated that due to the interdependencies and data exchanges that exist between reporting and nonreporting entities, CDT invited some nonreporting entities to participate in the first oversight life cycle. However, because nonreporting entities are not subject to CDT's oversight, CDT had gaps in the audit schedule when some opted not to participate. An information security audit and assessment manager (audit manager) explained that CDT spends several months preparing for each audit and thus cannot quickly pivot to an alternate entity when a scheduled entity declines to be audited. These gaps, along with delays in completing audits it does perform, resulted in CDT averaging just 10 of the 13 planned audits per year. Thus, without implementing any changes, CDT would need well over a decade to objectively assess all 108 reporting entities and establish the State's information security status.

Because CDT's ability to calculate maturity metric scores has been hindered by its slower-than-anticipated progress in completing compliance audits, we expected that it would be open to implementing staffing changes that would allow it to increase its capacity to complete audits. However, the state chief stated that CDT intends to keep the same goal of auditing 52 entities during each four-year oversight life cycle and does not have any immediate plans to hire more auditors or repurpose existing staff, which he believes would negatively impact its other operations. Rather, he explained that CDT relies in part on the results of the independent security assessments to gain assurance that the high-risk entities it has yet to audit will be able to mitigate immediate threats to their information security. However, as we discuss later, reporting entities have not demonstrated sustained improvements on the independent security assessments.

The state chief believes that implementing a proposed IT project will allow CDT to more efficiently conduct its audits. However, successfully implementing a new IT project can take years. Moreover, the state chief explained that the IT project has recently stalled because of funding constraints. If understanding the State's current information security status is paramount to implementing effective improvements—as CDT asserts—then it is taking a great risk by maintaining the status quo and waiting so long to determine what types of information security deficiencies may exist across the State.

CDT is taking a great risk by maintaining the status quo and waiting so long to determine what types of information security deficiencies may exist across the State.

Moreover, CDT is currently unable to calculate maturity metric scores for nearly one-third of the entities for which it has completed compliance audits. Specifically, for nine of 31 entities that it audited, it cannot calculate maturity metric scores because it did not assess the entities on all the required criteria. CDT designed the maturity metrics scoring methodology based on a recent revision to the NIST 800-53 standards that included a greater focus on privacy controls, such as limiting the amount of personal information collected and monitoring the use of the information. Although CDT formally adopted the maturity metrics scoring methodology in March 2018, it had yet to revise its audit program to reflect the new criteria for privacy controls when it began its four-year oversight life cycle in July 2018.

According to one of CDT's audit managers, implementing changes to its audit program and training its staff typically take a minimum of six months, and CDT does not generally make the changes effective until the following fiscal year audit cycle. She explained that the updated audit program reflecting the privacy controls consequently did not go into effect until fiscal year 2019–20. To maintain consistency in its comparison across state entities, CDT intends to calculate maturity metric scores only for entities that it has evaluated on the complete set of criteria.

According to the metrics manager, CDT is exploring two options for calculating maturity metric scores for these nine entities. Specifically, he explained that CDT may opt to perform a separate evaluation of the privacy controls for these entities so that they will be eligible to receive a maturity metric score. Alternatively, it may decide to develop a legacy maturity metric scoring methodology that excludes the privacy controls. It would then use this legacy methodology to recalculate maturity metric scores for all entities to facilitate a consistent comparison. Regardless of which option it chooses, the metrics manager stated that CDT intends to calculate the new maturity metric scores by June 2022.

Finally, as we describe in the Introduction, the second component of the maturity metrics are the independent security assessments that the Military Department typically completes. State law requires that no fewer than 35 reporting entities receive an independent security assessment each year. We performed an analysis for 2019 and 2020 and determined that CDT ensured that at least 35 reporting entities received an assessment in each of these years. Consequently, the independent security assessments have not contributed to CDT's delays in calculating reporting entities' maturity metrics.

The Military Department's independent security assessments have not contributed to CDT's delays in calculating reporting entities' maturity metrics.

CDT Does Not Use the Results of the Nationwide Review to Inform the Status of the State's Information Security

CDT requires reporting entities to participate in the yearly nationwide review because it is a condition of receiving information security grant funding from the U.S. Department of Homeland Security. The state chief explained that greater participation among state entities helps to maximize information security grant funding to the State. Because the nationwide review provides an overall assessment of each reporting entity's information security status, CDT could hypothetically use it to inform the status of information security in California. The manager of CDT's security risk governance unit stated that CDT records the nationwide review scores it receives from the federal government for each entity and notes any changes from year to year. However, she explained that CDT does not place much value on these results, and therefore, does not aggregate this information to identify statewide trends.

The state chief explained that CDT has little confidence in the nationwide review because each entity's results are based on self-reported information, which is subject to misrepresentation. For example, he stated that some entities may intentionally rate their information security maturity level as lower than it actually is in hopes of securing more federal grant funding. CDT indicated that because of its concerns over the accuracy of information that entities report on the nationwide review, it prefers to use independently verified information, such as its compliance audits and the Military Department's independent security assessments, to establish the overall status of the State's information security.

When we analyzed the reporting entities' performance on the nationwide review, we found that they have, on average, rated themselves slightly below the federally recommended minimum level of 5. Further, they have remained stagnant in their information security development. Specifically, the State's average score remained nearly unchanged from 2018 through 2020, only increasing from 4.92 to 4.93. These scores indicate that although the reporting entities have established formal policies to guide their cybersecurity activity, they are still in the process of developing standards and procedures that would allow for consistent implementation of their identified information security practices. In the absence of consistent implementation, the entities lack assurance that their information security controls are operating as they intend and thus meeting established security and privacy requirements.

The State's average score on the nationwide review remained nearly unchanged from 2018 through 2020.

This lackluster performance is not unique to California; the federal government reported that the nationwide average score across all 50 states was 4.88 for 2020, which is the most recently published national metric. Nonetheless, the analysis we performed using information that is readily available to CDT demonstrates that the State continues to perform at a substandard level and has failed to make any significant improvement to its information security over the last three years. By deciding not to place more value in the nationwide review scores, CDT is ignoring a source of comprehensive, potentially useful data regarding the State's information security. Further, as we discuss in the following section, its concerns regarding entities understating their performance are unfounded. Although we agree that independently verified information is preferable, CDT's failure to sufficiently implement its compliance audits has left the State without a clear picture of the status of its information security. CDT could use the nationwide review scores to help focus that picture.

Finally, not only could CDT use the results of the nationwide review to gain perspective on the State's information security status, it could also leverage this information to help the State improve. Specifically, the federal government provides resources and guidance to assist entities with using their nationwide review results to identify potential next steps toward cybersecurity improvements. Upon completion of the nationwide review, the federal government gives entities access to custom reports that include details on each information security control category so that the entities can identify actionable steps to improve their cybersecurity maturity. It has also developed cross-references to best practices, standards, and requirements related to each control category that entities can use to help develop their information security. Until CDT develops a better approach to oversight of information security, it should utilize these resources to identify the most common information security deficiencies across the State and provide targeted guidance to reporting entities to help them remediate those outstanding issues. Doing so could allow the State to make a significant step forward in improving its information security.

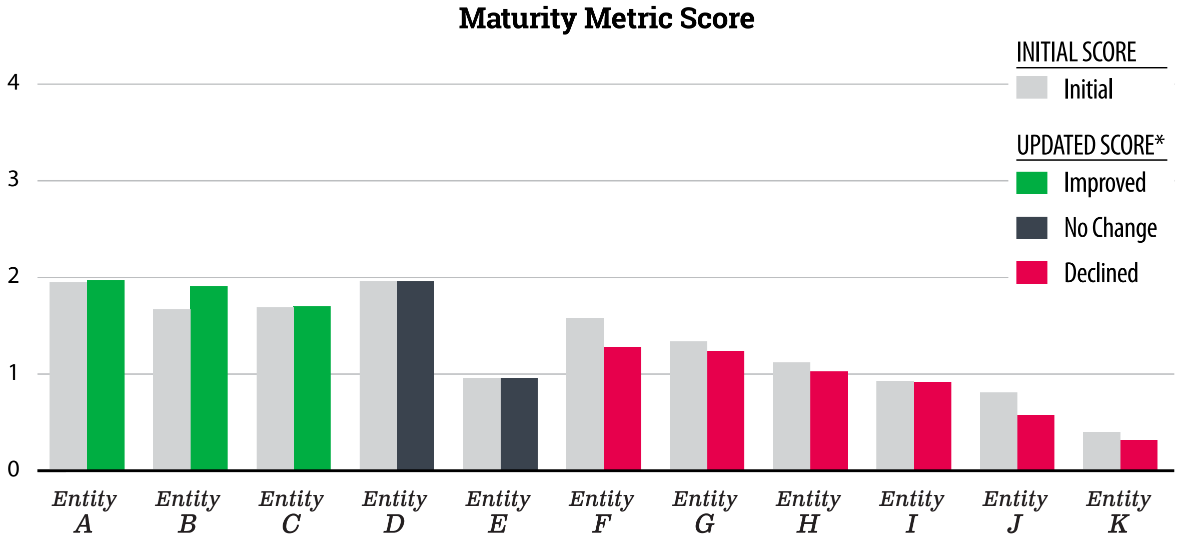
CDT could use the results of the nationwide review to gain perspective on the State's information security status and to help the State improve.

The Information CDT Has Collected Indicates That Reporting Entities Continue to Perform Below Recommended Standards

Although CDT has not established an overall information security status for the State, the information it does have shows that reporting entities are not making sufficient progress in their information security development. As of the end of the third year of the oversight life cycle in June 2021, CDT had calculated maturity metric scores for 17 reporting entities and found that they achieved an average maturity metric score of 1.3. Although the maturity metrics utilize a scale of 0 to 4, CDT has not identified a minimum score that entities should strive to achieve. The 17 reporting entities' average score of 1.3 means that they have developed the foundational elements of their information security program—such as an inventory of their information assets and information security policies—but are still in the process of developing practices and procedures to put those foundational elements into action. In fact, on average, these entities performed even worse on CDT's maturity metric than what they self-reported on the nationwide review, undercutting CDT's concern that they might have understated their information security status when reporting to the federal government.

Eleven of the 17 reporting entities subsequently received either a follow-up review or another independent security assessment, allowing CDT to update their maturity metric scores to measure their progress. As Figure 8 shows, the results are not encouraging. Only three of the 11 entities showed any improvement, and it was minimal. Another two entities earned an exact repeat of their initial scores, and six entities saw their scores decline. We would not necessarily expect sharp improvements in the entities' information security development because securing resources and implementing corrective action to address identified deficiencies takes time. However, we are concerned to see that some entities actually performed worse on their subsequent assessments, despite increased oversight of their information security programs.

Figure 8
The Updated Maturity Metric Scores for 11 Reporting Entities Show Little or No Progress



Source: CDT's maturity metric scores.

Note: In an effort to protect the State's information assets, we have chosen not to publicly disclose the names of the reporting entities. As a result, we assigned each of these reporting entities a letter.

* On average, CDT calculated the updated maturity metric scores for these 11 reporting entities approximately one year after calculating their initial scores.

Similarly, scores on the independent security assessments the State has performed have remained stagnant. The State has completed more independent security assessments to date than compliance audits, and the assessments have covered far more entities and include some nonreporting entities. We analyzed 135 independent security assessments completed from January 2018 through March 2021 and found that, on average, state entities achieved a score of 54 out of 100. The Military Department identifies a score of 90 or higher as the desired range for entities to achieve, which means that the State's average score is far below the desirable level. Further, the State's progress remained relatively flat, starting with an average score of 52 during the first year before increasing slightly during the middle two years, only to drop back down to an average score of 52 in the first three months of the final year. Although the state chief asserted that entities have demonstrated improvement in certain areas of the assessments, such as phishing click rates and resiliency to external compromise, they have not made enough progress across all the control categories to drive improvement in their overall information security assessment scores.

The state chief acknowledged that because of the poor performance of the entities that CDT has evaluated in its first four-year oversight life cycle, it intends to carry over about one-third of them to the next four-year life cycle, which begins in fiscal year 2022–23. He explained that these entities remain a high risk and have not made enough progress for it to cease close monitoring of them. Not only does this decision demonstrate that the entities in question are not making sufficient progress in developing their information security, it will also delay CDT's efforts to provide evaluation and monitoring of the reporting entities it has yet to audit.

Although CDT has information from multiple sources that shows the State's information security status is poor, it has not shared this information with the Legislature. The state chief explained that CDT generally participates in quarterly briefings with the Legislature. He asserted that the briefings address information such as the statewide status of plan of action documents, general emerging threats to the State's information security, and issues it needs help with from a policy standpoint. We reviewed CDT's presentations and found that it shared high-level information with the Legislature about its compliance audits, such as the number of findings it had issued and the most common control categories in which it had identified high-risk findings. However, CDT generally did not share more detailed information—such as the results of the nationwide review and the maturity metric scores it has calculated—that would have provided the Legislature with a more comprehensive picture of reporting entities' information security statuses. In the absence of complete information, the Legislature lacks perspective on the significant weaknesses that exist in the State's information security and thus cannot take appropriate steps to hold CDT and reporting entities accountable.

CDT generally did not share the type of detailed information that would have provided the Legislature with a more comprehensive picture of reporting entities' information security statuses.

CDT Does Not Adequately Follow Up to Ensure Entities' Timely Compliance With Self‑Reporting Requirements

CDT requires reporting entities to engage in self-reporting mechanisms to demonstrate that they are aware of the State's information security and privacy requirements, and of their deficiencies they have yet to address. However, it does not adequately follow up with the entities to ensure timely compliance with its reporting requirements. As we explain in the Introduction, CDT requires reporting entities to submit an annual compliance certification. In this document, the director or equivalent head of the reporting entity acknowledges awareness both of any identified risks and of the need to address these deficiencies to ensure compliance with the State's information security and privacy requirements.

However, CDT has not performed sufficient follow-up to ensure that all reporting entities comply with this requirement. The state chief explained that the compliance certification holds the head of each reporting entity accountable for the entity's information security status. However, 18 of the 108 reporting entities had failed to submit compliance certifications as of March 2021. On average, these 18 entities were more than two years overdue in submitting their compliance certifications, and four had never submitted one. Although CDT sends reminder emails to reporting entities, this approach has not been effective. If it does not ensure that reporting entities submit their compliance certifications, it cannot demonstrate that they are aware of the importance of information security and of their responsibility for making continued improvements. CDT is consequently in a weakened position to hold them accountable.

Even though reporting entities agree in their annual compliance certifications that they will perform self-assessments of their critical IT systems, they have completed very few to date. CDT requires reporting entities to perform a self-assessment for each of their critical IT systems, culminating in a high-risk findings report that they must submit to CDT. According to CDT's risk reporting user guide, these self-assessments allow reporting entities to evaluate their critical IT systems for potential security risks and establish plans to resolve or mitigate those risks. However, a 2020 statewide analysis that CDT conducted showed that reporting entities had completed self-assessments for only 172 of their nearly 3,300 critical IT systems. For example, an entity that is responsible for a large number of critical IT systems in the State had assessed only 10 percent of them. Further, the count of the State's critical IT systems is incomplete because CDT's analysis shows that 17 percent of reporting entities had yet to report the total number of critical IT systems for which they are responsible.

A 2020 statewide analysis that CDT conducted showed that reporting entities had completed self-assessments for only 172 of their nearly 3,300 critical IT systems.

One reporting entity explained that the concept of what constitutes a critical IT system is vague. The state chief echoed this sentiment, acknowledging that entities' different interpretations of how to prioritize and define a critical system has presented a challenge. He explained that some entities are exhaustive in their count of critical IT systems and report all of the individual subcomponents within a main system, whereas others remain at a high level and just report the single, main system. Nonetheless, CDT has yet to provide clear direction on what constitutes a critical IT system and how to perform the count. In addition, one reporting entity we interviewed explained that it experienced several challenges in using the self-assessment tool. Although it worked with CDT to try to resolve them, it ultimately gave up on the self-assessment process after assessing only a portion of its critical IT systems. The state chief acknowledged that CDT has received feedback from other entities that the self-assessments are burdensome and do not seem to be useful.

CDT has received feedback that self-assessments are burdensome and do not seem to be useful.

Most troubling, the state chief stated that CDT also does not find much value in the current self-assessment tool because it is based upon self-reported information, which CDT believes is subject to misrepresentation. He stated that CDT is considering implementing a more effective self-assessment tool as part of the larger proposed IT project. However, as we previously discuss, CDT has yet to secure funding for this system and thus does not have a timeline for how soon it will be implemented.

Despite the challenges that reporting entities have identified with the self-assessment process and the fact that CDT is not utilizing the information the process produces, the state chief stated that CDT is still encouraging entities to assess their critical IT systems if they have the time and resources to do so. However, he explained that CDT has placed more emphasis on guiding entities to focus on remediation efforts—such as addressing outstanding items on their plans of action—instead of reporting activities. Given that the self-assessments are supposed to aid entities in identifying such outstanding information security risks for their plans of action, we disagree with CDT's approach.

Moreover, by not making self-assessments a priority, CDT is not only missing an opportunity to proactively help reporting entities prevent security breaches, it is limiting its own ability to use their plans of action to identify common issues that may exist across the State's critical IT systems. As we discuss in the Introduction, a reporting entity should regularly update its plan of action with a list of its information security deficiencies and its plans for remediating those deficiencies. CDT requires reporting entities to submit their plans of action on a quarterly basis to update it on their progress. It then compiles the plan of action documents across all state entities to calculate statewide statistics, such as the top NIST 800-53 control categories for which the State has outstanding issues. CDT's risk manager states that this information helps it to identify specific areas where entities may need additional training.

Nonetheless, CDT has failed to ensure that all reporting entities submit complete plans of action. Specifically, 15 of the 108 reporting entities were overdue in submitting their plans of action as of March 2021. Although these entities were typically only one quarter overdue with their submissions, we observed five entities that were a year or more overdue and another entity that had never submitted a plan of action to CDT. Further, many of the plans of action that entities did submit were incomplete because CDT did not ensure that they performed all the required self-assessments of their critical IT systems. By performing its statewide analysis on incomplete plans of action, CDT lacks assurances that it is focusing its information security oversight efforts on the areas that pose the highest risk to the State.

CDT lacks assurances that it is focusing its information security oversight efforts on the areas that pose the highest risk to the State.

CDT Failed to Complete Timely Updates to the Information Security Standards With Which Reporting Entities Must Comply

As the Introduction explains, the State has adopted NIST 800-53 as its minimum information security controls. Nonetheless, CDT waited nearly a year to begin updating the information security and privacy policies it prescribed in SAM 5300 and SIMM to reflect current NIST standards. Specifically, the federal government released a draft revision to NIST 800-53 in August 2017 for public review and comment. As we discuss previously, CDT relied upon the draft NIST standards in developing the methodology it published in March 2018 for calculating maturity metric scores. Therefore, CDT has known that a revision to NIST 800-53 was forthcoming since at least 2018. However, it did not hire someone to assist with updating the State's policies until nearly a year after the federal government published the most recent version of NIST 800-53 in September 2020.

According to CDT's security manager, the updates to SAM 5300 and SIMM constitute a major overhaul for CDT, and the individual completing the updates must have extensive security policy knowledge. She explained that the manager of CDT's security risk governance unit—who is CDT's expert on SAM 5300 and SIMM—had historically handled most of the policy updates. However, the security risk governance manager was unable to complete the updates because she was too busy with other assignments. Nonetheless, by failing to be more proactive with its planning, CDT caused significant delays to updating SAM 5300 and SIMM so they reflect the most current NIST 800-53 standards.

In the meantime, the current versions of SAM 5300 and SIMM continue to direct reporting entities to an outdated version of the federal information security standards with which they are required to comply. This is especially concerning because, as the federal government explains, new safeguards and countermeasures are needed to protect the critical and high-value assets of organizations against rapidly evolving cyberthreats. The federal government states that it added new controls to NIST 800-53 based on the latest threat intelligence and cyberattack data, such as supply chain risk management. If CDT does not complete timely updates to SAM 5300 and SIMM, it cannot ensure that entities are aware of new controls that are intended to support their cyber resiliency and strengthen their security and privacy governance, among other things.

The Recent Increase in Telework Has Created New Information Security Risks for Reporting Entities That CDT Must Continue to Address

State entities are at higher risk when employees telework—even if employees are using devices and computers that the entity has provided. NIST advises that telework can result in a lack of physical security controls; the potential use of at-risk technology, such as unsecured networks; the connection of infected devices to entity data systems; and the exposure of internal information assets to unknown external threats. One of the primary threats of telework is malware, which can infect devices through many means, including email and websites. NIST cautions that an organization should assume that technologies used for teleworking contain hostile threats that will attempt to gain access to the organization's data and resources. According to IBM Security, in 2021 the average total cost of a data breach ranged from $1.9 million for the public sector up to $9.2 million for the health care industry. Moreover, the unauthorized release of sensitive information can damage the public's trust in an entity, jeopardize its mission, and harm individuals whose personal information has been released.

If state entities permit the use of personal devices outside of their control, it creates additional security concerns. Personal devices, which users manage themselves, are typically not secured to the same degree as the devices belonging to state entities. The text box shows examples of the steps state employees can take to mitigate the risks of using a personal device. However, some of these steps may be challenging for many employees to implement. As a result, unsecured, malware-infected, and otherwise compromised devices may end up connected to sensitive state resources.

Steps for Securing a Personally Owned Computer for Telework

- Use a combination of security software, such as antivirus software, personal firewalls, spam and web content filtering, and pop-up blocking.
- Apply updates to the operating system and applications, including web browsers, email clients, instant messaging clients, and security software.
- Disable unneeded networking features.
- Install and use only known and trusted software.
- Configure remote access software based on the entity's requirements and recommendations.
- Restrict who can use the personal computer with separate user accounts and prevent unauthorized physical access.
- Maintain security on an ongoing basis by using strong passwords.

Source: NIST *User's Guide to Telework and Bring Your Own Device (BYOD) Security.*

CDT took emergency steps at the beginning of the pandemic to help reporting entities prepare for an increase in teleworking. For example, it surveyed them to determine their readiness for widespread teleworking and coordinated with the Military Department to conduct abbreviated security assessments to assist them in securing the networks they used for telework. CDT then followed up on the Military Department's critical findings to monitor their resolution. CDT also sent out mass emails to reporting entities with security guidance about telework, including an emergency telework guide. In addition, CDT created a website that addresses telework best practices and information security, which serves as the State's online *California State Telework Guide*. When we followed up with five reporting entities, we found that they generally had appropriate telework policies and trainings, and they directed employees to CDT's guidance.

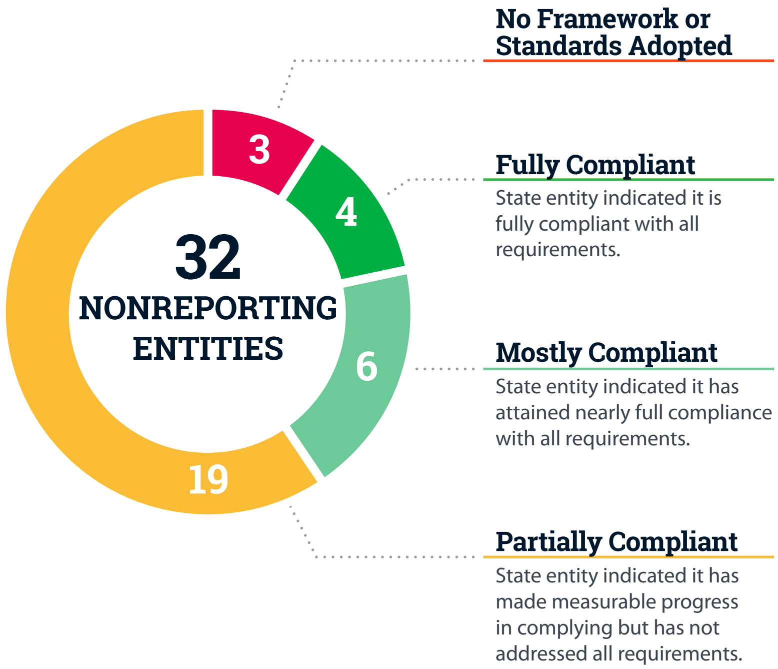
However, CDT's guidance related to the security of personal devices used for teleworking is not entirely clear. Specifically, guidance in SIMM describes steps employees should take to secure their personal devices used for telework. However, the text implies that these steps are only required in limited circumstances. When we followed up with CDT regarding this issue, it stated that the guidance applied to all personal devices and that it plans to update the language to make it clearer. By clarifying the specific steps that an employee must take to secure a personal device used for teleworking, CDT could help reporting entities ensure that their employees are taking appropriate security precautions.

By clarifying the specific steps to secure a personal device used for teleworking, CDT could help ensure that employees are taking appropriate security precautions.

Many Nonreporting Entities Are Not Fully Compliant With Their Information Security Standards

Although state law does not apply CDT's requirements to nonreporting entities, that fact does not diminish the critical necessity for nonreporting entities to safeguard their data and the systems that facilitate essential state services. We surveyed 32 nonreporting entities and found that 29 had adopted an information security framework or standards. However, as Figure 9 shows, only four of the 29 reported they had achieved full compliance with their chosen framework or standards. Further, although all 29 reported that they had obtained information security assessments, two had obtained their assessments more than three years ago; in the years that have since elapsed, critical weaknesses may have gone undetected. Moreover, nine of the 29 entities indicated that they will need three years to remediate the high-risk information security findings identified in their assessments. Finally, three of the 32 reported that they have not adopted any information security framework or standards.

Figure 9
Most Nonreporting Entities Stated That They Are Only Partially Compliant With Their Selected Security Standards

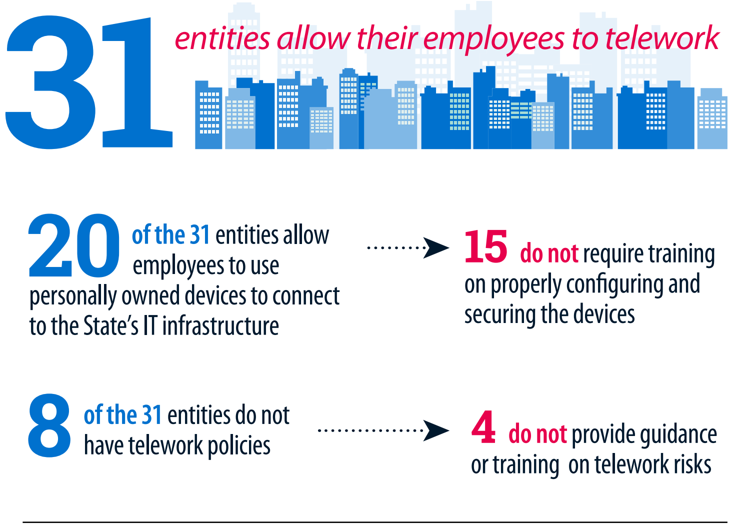


Source: Analysis of survey responses.

We also found that nonreporting entities have not been consistently providing telework security guidance or training to their employees, leaving them more vulnerable to security incidents. Of the 32 survey respondents, 31 reported that they allowed staff to telework. However, as Figure 10 shows, a quarter of those entities stated that they lacked telework policies related to information security. Further, although many of the nonreporting entities allow their employees to use personally owned devices to connect to the State's IT infrastructure, most stated that they did not require specialized training on properly configuring and securing those personal devices. While some nonreporting entities had not developed telework guidance and training because they generally had not allowed telework before the COVID-19 pandemic, we would expect them to have since developed the guidance necessary to ensure information security.

We performed an additional review of five nonreporting entities, three of which asserted in our survey that they had telework policies and procedures related to information security and two of which stated that they lacked telework policies and procedures. As they had reported, the three generally had telework policies and training that met state telework standards, while the other two had some policies and training in place that fell short of the state telework standards.

Figure 10
Although Nearly All of the Nonreporting Entities We Surveyed Offer Telework to Their Employees, Many Lack a Telework Policy



31 *entities allow their employees to telework*

20 of the 31 entities allow employees to use personally owned devices to connect to the State's IT infrastructure → 15 do not require training on properly configuring and securing the devices

8 of the 31 entities do not have telework policies → 4 do not provide guidance or training on telework risks

We surveyed 32 nonreporting entities, and only one did not allow its employees to telework.

Source: Analysis of survey responses.

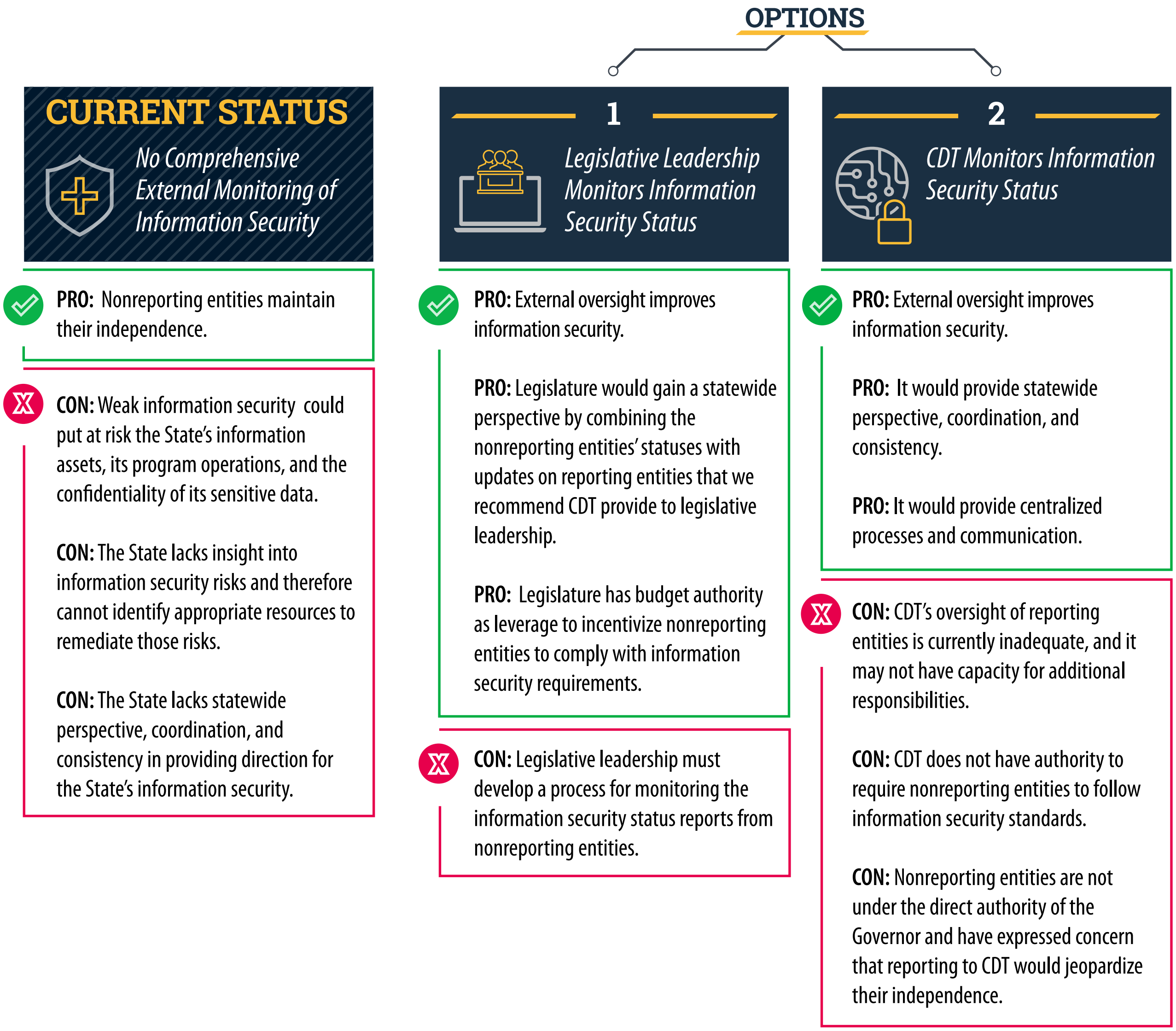
In our July 2019 report, we found that gaps in oversight had contributed to nonreporting entities' information security weaknesses.[3] We noted that some nonreporting entities are subject to an external oversight framework that requires them to regularly assess their information security and that these entities assessed more of their selected information security standards than those that had no such requirement. We concluded that without the accountability that external oversight provides, nonreporting entities may be less likely to resolve information security issues in a timely manner. Although our analysis demonstrated the value of establishing an oversight framework for nonreporting entities, most of the nonreporting entities we reviewed for our July 2019 report asserted that they did not have such a framework.

In light of our previous conclusion that external oversight improves a state entity's information security status and of our survey results indicating that most nonreporting entities are not fully compliant with their chosen information security framework or standards, we recommend that the Legislature create an oversight framework for nonreporting entities. As Figure 11 shows, one option would

[3] *High Risk Update—Information Security: Gaps in Oversight Contribute to Weaknesses in the State's Information Security,* Report 2018-611, July 2019.

be for CDT to monitor the information security status of nonreporting entities. However, as we noted in our prior report, several nonreporting entities have expressed concern that reporting to CDT would jeopardize their independence. In addition, we identified multiple issues with CDT's current oversight of reporting entities, and we question whether CDT has the capacity to monitor nonreporting entities.

Figure 11
An External Oversight Framework Would Provide Increased Assurance of Nonreporting Entities' Information Security



OPTIONS

CURRENT STATUS
No Comprehensive External Monitoring of Information Security

✓ **PRO:** Nonreporting entities maintain their independence.

✗ **CON:** Weak information security could put at risk the State's information assets, its program operations, and the confidentiality of its sensitive data.

CON: The State lacks insight into information security risks and therefore cannot identify appropriate resources to remediate those risks.

CON: The State lacks statewide perspective, coordination, and consistency in providing direction for the State's information security.

1
Legislative Leadership Monitors Information Security Status

✓ **PRO:** External oversight improves information security.

PRO: Legislature would gain a statewide perspective by combining the nonreporting entities' statuses with updates on reporting entities that we recommend CDT provide to legislative leadership.

PRO: Legislature has budget authority as leverage to incentivize nonreporting entities to comply with information security requirements.

✗ **CON:** Legislative leadership must develop a process for monitoring the information security status reports from nonreporting entities.

2
CDT Monitors Information Security Status

✓ **PRO:** External oversight improves information security.

PRO: It would provide statewide perspective, coordination, and consistency.

PRO: It would provide centralized processes and communication.

✗ **CON:** CDT's oversight of reporting entities is currently inadequate, and it may not have capacity for additional responsibilities.

CON: CDT does not have authority to require nonreporting entities to follow information security standards.

CON: Nonreporting entities are not under the direct authority of the Governor and have expressed concern that reporting to CDT would jeopardize their independence.

Source: State Auditor analysis.

Another option is for the Legislature to monitor the information security status of nonreporting entities by requiring them to perform or obtain an audit of their information security status every three years and to provide confidential annual updates regarding their status to legislative leadership, including the majority and minority leaders of the State Senate and the State Assembly. This option would establish external information security monitoring that both preserves the confidentiality of specific information security risks and ensures greater independence for nonreporting entities. Without a new oversight framework for nonreporting entities, the status quo—which provides no comprehensive external monitoring of nonreporting entities' information security status—will continue.

Recommendations

Legislature

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

- Require that CDT confidentially submit an annual statewide information security status report, including the maturity metric scores it has calculated and the results of the nationwide review, to the appropriate legislative committees no later than December 2022. This status report should include CDT's plan for assisting reporting entities in improving their information security.

- Require each nonreporting entity to adopt information security standards comparable to SAM 5300 and to provide a confidential, annual status update on its compliance with its adopted information security standards to legislative leadership, including the president pro tempore of the California State Senate, the speaker of the California State Assembly, and minority leaders in both houses. It should also require each nonreporting entity to perform or obtain an audit of its information security no less frequently than every three years.

- Require nonreporting entities that allow employees to telework to develop telework policies and training comparable to those CDT requires.

CDT

To ensure that it understands the statewide security status of reporting entities, CDT should do the following:

- Increase its capacity to perform timely compliance audits of high-risk entities, which may entail hiring more staff or securing additional contracted audit support. Further, CDT should prioritize calculating maturity metric scores for the nine entities that it has audited but that do not yet have scores because it has not evaluated their privacy controls. CDT should complete these steps by the conclusion of the four-year oversight life cycle in June 2022.

- Until it is able to conduct timely, objective audits of reporting entities, CDT should provide additional guidance to them by April 2022 on what constitutes a critical IT system and follow up annually to ensure that they complete the required self-assessments of those systems.

- Utilize the information from the entities' self-assessments of their systems, as well as from the nationwide review, to annually help identify common areas that require improvement across multiple reporting entities.

To help ensure that reporting entities are aware of new federal information security standards that are intended to strengthen their security and privacy governance, CDT should complete the necessary updates to SAM 5300 and SIMM by June 2022.

To help reporting entities ensure that their teleworking employees are taking appropriate security precautions, CDT should clarify guidance by February 2022 to require all employees using personal devices for state business to implement baseline security measures.

We conducted this performance audit in accordance with generally accepted government auditing standards and under the authority vested in the California State Auditor by Government Code section 8543 et seq. 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 the audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Respectfully submitted,

Michael Til

MICHAEL S. TILDEN, CPA
Acting California State Auditor

January 18, 2022

Blank page inserted for reproduction purposes only.

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 we identify as being at high risk for the potential of waste, fraud, abuse, and mismanagement or as having major challenges associated with its economy, efficiency, or effectiveness. In August 2021, we issued our latest assessment of high-risk issues that the State and selected agencies face. Because we continue to identify information security as a high-risk issue for the State, we performed this audit to evaluate CDT's efforts to help improve the information security of reporting entities. We also evaluated whether nonreporting entities have complied with their selected information security standards. We list the objectives we developed and the methods we used to address them in the following table.

Audit Objectives and the Methods Used to Address Them

	AUDIT OBJECTIVE	METHOD
1	Review and evaluate the laws, rules, and regulations significant to the audit objectives.	Reviewed relevant laws, regulations, and other background materials.
2	Evaluate CDT's oversight of reporting entities' information security, including its progress in establishing an information security baseline status for reporting entities.	• Interviewed CDT staff to gain an understanding of the assessments it conducts or obtains to evaluate the reporting entities' information security status. • Reviewed CDT's audit program and the results of its assessments.
3	Determine whether reporting entities' compliance with information security standards has improved.	Evaluated the nationwide review results and CDT's maturity metric scores for reporting entities.
4	Evaluate the measures and guidance CDT has developed to address the increased security risk due to the number of state employees who are now teleworking as a result of the COVID-19 pandemic. For a selection of reporting entities, determine the measures taken to address telework risks and whether they comply with CDT's guidance. Finally, determine whether there has been an increase in reported information security incidents during the pandemic.	• Reviewed and evaluated the measures CDT took and the guidance it provided to reporting entities to address the risks related to telework. • Selected five reporting entities for review based on their responses to specific questions on a survey CDT conducted, such as how many teleworking employees they have and whether they have telework policies. • Interviewed staff at each of the five selected entities to gain an understanding of their information security practices related to telework. • Obtained and reviewed the information security policies, training, and guidance the entities provided to teleworking employees. • Reviewed CDT data related to security incidents and found that the number of reported incidents did not significantly change after the start of the pandemic.

continued on next page . . .

	AUDIT OBJECTIVE	METHOD
5	Determine whether nonreporting entities have improved their compliance with their selected information security standards. Evaluate their efforts to mitigate teleworking risks and determine whether there has been an increase in information security incidents during the pandemic.	• Conducted a survey of nonreporting entities related to their compliance with selected information security standards and telework. We also asked about security incidents related to telework that occurred since March 2020 and found that more than 80 percent of survey respondents did not report any incidents. • Selected five nonreporting entities based on certain factors from their survey responses, such as how many teleworking employees they have and whether they have telework policies. – Interviewed staff at selected entities to gain an understanding of their information security practices related to telework. – Obtained and reviewed the information security policies, training, and guidance the entities provided to teleworking employees.
6	Review and assess any other issues that are significant to the audit.	We did not identify any other issues of significance.

Source: Audit workpapers.

Assessment of Data Reliability

The U.S. Government Accountability Office, whose standards we are statutorily obligated to follow, requires us to assess the sufficiency and appropriateness of computer‑processed information we use to support our findings, conclusions, or recommendations. In performing this audit, we relied on various spreadsheets we obtained from CDT. To evaluate these data, we reviewed existing information about the data, interviewed staff members knowledgeable about the data, and performed testing of the data. As a result of this testing, we found the data were sufficiently reliable for our audit purposes.

STATE OF CALIFORNIA GAVIN NEWSOM, Governor

CALIFORNIA DEPARTMENT OF TECHNOLOGY
P.O. Box 1810
Rancho Cordova, CA 95741-1810
(916) 319-9223

Amy Tong, Director
Russell Nichols, Chief Deputy Director

December 17, 2021

Elaine Howle (via GovOps Agency Secreta Yolanda Richardson)*
California State Auditor
621 Capitol Mall, Suite 1200
Sacramento, CA 95814

SUBJECT: 2021-602 – STATE HIGH RISK UPDATE – INFORMATION SECURITY

Dear Ms. Howle:

California Department of Technology's (CDT) Opening Comments:

The California Technology Department appreciates the California State Auditors' collaborative effort in providing valuable insight into scaling oversight to mature the security posture of all State entities. In the wake of the pandemic the cybersecurity threat landscape nearly quadrupled in the sophistication of attacks by nation state adversaries and criminal rings targeting every layer of our critical infrastructure. CDT anticipated this threat, immediately scaled up and supported technology based pandemic response and remote work enablement. Efforts included helping State entities implement systems to support Covid-19 management, contact tracing, vaccine distribution, and guidance on telework best practices. We acknowledge the State must further invest into additional measures to be resilient against the threat. The pandemic has upended the conventional standards for evaluating cybersecurity metrics. The threat landscape has evolved from the traditional cybersecurity breaches such as DDOS attacks to sophisticated ransomware attacks and identity theft. CDT is in process of revaluating the metrics in the context of the cybersecurity ecosystem as it exists today. CDT has been cognizant of its oversight responsibilities even while pandemic response has taken priority over compliance audits.

It is important to note, that while compliance audits were re-prioritized during the ① pandemic, the Information Security Assessments conducted by the California Military Department (CMD) continued on schedule. In addition, CDT in partnership with CMD conducted 92 Rapid Assessment for Cybersecurity Exposure (RACE) against state entities to ensure they are adequately prepared and detect vulnerabilities in their information technology (IT) infrastructure as they quickly transitioned to telework.
CDT has played a significant role in developing and establishing California Cybersecurity Integration Center (CalCSIC) to provide a centralized advanced security monitoring

* California State Auditor's comments begin on page 45.

capability to augment state entities. CalCSIC provides a dedicated threat intelligence and response team to assist state entities respond to immediate threats, resulting from sophisticated ransomware, supply chain attacks, and sophisticated identity theft.

Notably, in 2021, the CDT shifted the Security Operations and Audit cost funding model, to allow state entities to retain funding for internal remediation efforts. To sustain our defense posture, proactive measures in CDT's oversight and governance abilities need to further scale.

Additionally, and more importantly, the Cal-Secure roadmap released in October of 2021 outlines the path forward and the recommended input outlined in this report reinforces the reasoning and support for roadmap efforts. With the release of Cal-Secure roadmap and the modifications to the cost funding model, CDT has developed a path for the State entities to achieve increased cyber maturity.

The following are the Agency Comments in response to the Areas of Concern presented in the Draft State High Risk Update Report:

1. **CDT's Four-Year Oversight Life Cycle is not sufficient to assess the status of the State's Information Security:**

The four-year cycle is specifically intended and designed to assess high-risk departments running the most critical and impactful services. The cycle encompasses comprehensive policy audits as well as technical vulnerability assessments for high-risk entities.

Pursuant to Government Code section 11549.3 (g), CDT has broad authority and discretion under the statute determine the entities subject to compliance audits. Low-risk entities are excluded from the four-year compliance audit cycle. CDT monitors low-risk entities through other mechanisms such as periodic CMD independent security assessments and tracking and remediation through the Plan of Action and Milestone (POAM) process. Additionally, to-date nearly 30 entities have been onboarded to the SOC for enhanced monitoring and support.

The draft report has a number of factual inaccuracies related to the number of high-risk entities and the number of complete compliance audits. Specifically,

② - The number of high-risk entities identified at the beginning of the four-year cycle fluctuates. Our policy, which is spelled out in CalSecure, is to determine the list of high-risk entities to be audited and is based on an algorithm to determine entity impact to the citizens of the state and other factors. Important to note that the 52 audits over four-year cycle was a self-imposed target based on factors considered 4 years ago. We are currently on target to complete 48 audits even under the

circumstances of the pandemic and reprioritization of compliance audits. This is a ③
92% success rate. The four entities have specifically claimed to be exempt from
CDT's information security oversight authority for this cycle.

- <u>10 -13 audits per year is an annual average</u>. As CSA acknowledges, CDT has
completed 31 of 39 audits. According to SIM 5300-C, the high-risk designation is
subject to change based on various factors, such as the type of data that entities
store, the nature of their business, the maturity of their overall information security
programs, and their likelihood of facing threats that necessitate a high level of
attention and monitoring. Accordingly, 8 entities were accommodated for ①
scheduling purposes because of pandemic or were reprioritized based on maturity.
As of today, we are on track to complete 48 high risk entities. During the pandemic,
and upon request of the entities themselves, CDT prioritized the RACE assessments
and completed 92 such assessments within a relatively short time.

- CSA estimated that it would take CDT 12 years to audit 108 entities wholly is ④
inaccurate and irrelevant. As described above, the intent was never to audit all
108 entities. CDT has always focused on high-risk entities rather than a specific
number of entities. Therefore, Figure 2 is misleading. ⑤

- The report is also misleading to the extent it states that entities scores were not
calculated based on required criteria. As the threat landscape changes, the audit
controls are updated between audit cycles. New controls and criteria were added ⑥
and were not included in the original audit scope to account for these new threats.

- Finally, the report alludes to an IT Project on page 27, para 2. The project does not ⑦
currently exist but is a potential solution that the CDT is considering to augment
current tools.

2. CDT does not use the results of the Nationwide Review to inform the status of the State's Information Security:

This particular finding is purely CSA's opinion and is unrelated any particular performance ⑧
criteria that CDT's needs to comply with pursuant to statute or policy.

Third party self-assessment mechanisms such as the National Cyber Security Review
(NCSR) are self-reported, subjective, and not an accurate reflection of an entity's security
posture. NCSR score in particular, is not a credible or objective criteria for determining an ⑨
entity's cybersecurity maturity metrics. While CDT directs participation for purposes for
federal funding, CDT for reasons CSA acknowledges, does not leverage the subjective

scores. While the recommendation to take the NCSR scores into consideration is well received, this cannot be a finding against CDT and is irrelevant to the compliance audit of high-risk entities. Self-reporting by state entities is wholly beyond the control of CDT's compliance audit process.

While CDT has generally adopted NIST 800-53 is a minimum standard for the state entities, SAM 5300 clearly states that the CDT has implemented additional California specific standards. Pursuant to SAM 5300 - Entities shall ensure their security control selections and tailoring, at a minimum, comply with the State-defined Security Parameters for NIST SP 800-53 (SIMM 5300-A) and the prioritization of their information security program development and implementation align with the Foundational Framework for Information Security (SIMM 5300-B). Further, SIMM 5300-A is mapped to specific NIST 800-53 controls. Notably, not all NIST 800-53 controls have been adopted by CDT. While NCSR may be contained within the NIST framework, CDT has specifically not adopted the NCSR scores to measure maturity metrics.

⑩ As reporting methodologies and increased information sharing has enhanced with the federal entities supporting NCSR, the CDT will evaluate the merit of incorporating these self-assessment questionnaires into risk ranking processes. Regardless, self-reporting is not a reasonable metric to establish information security standards statewide and is not an appropriate finding for a performance audit.

3. **The Information CDT has collected indicates that reporting entities continue to perform below recommended standards:**

⑪ The threat landscape is continually evolving requiring new audit controls. Therefore, one audit period may adopt new or modify existing criteria and is not a direct comparison of the prior year. CDT plans to calculate and implement a difficulty factor which will normalize scoring year over year. While higher scores are generally preferred, the lower score of a subsequent period is not necessarily reflective of an entity's lack of progress. As CSA acknowledged, information security is a shared responsibility. The audit findings are intended inform state entities to further action to enhance their security posture. The scores also do not take into account the significant security operational assistance provided through statewide services such as Statewide Security Operations Center and Cal-CSIC.

⑫ The Legislature reporting statement is inaccurate. During the audit period, CDT provided a number of comprehensive security briefings to the Legislature ensure they are fully informed about the evolving threats and status of state entities.

4. Although many reporting Entities Information Security is below Standards, CDT has not taken critical steps to help them improve:

The audit, and this finding in particular overlooks the significant measures that CDT has ⑬ implemented to bolster the state's operational security posture. As mentioned, compliance audits are but a small subset of the overall efforts.

The CDT operationalized a Statewide Security Operations Center intended to monitor and protect all state entities. CDT plans to add additional security as a service capability as outlined in Cal-Secure to assist entities with security measures that cannot be achieved locally.

We acknowledge State entities need to make faster progress in mitigating CDT identified findings. The CDT has taken recent actions such as:

- In response to the pandemic and scaling up the States remote workforce, CDT with the joint Cal-CSIC teams conducted over 92 RACE assessments on remote work technologies and aided entities in remediating security deficiencies,
- Require all entities to successfully adopt and integrate advance Endpoint Protection and Detection capabilities.
- Coordinated mitigation, remediation, and response to complex global cyber chain cyber events resulting from Solarwinds,
- Instituted centralized services such as the Security Operations Center (SOC),
- Establish a dedicated incident response team operating within the Cal-CSIC which aided State entities with complex incident response and fraud investigation supporting entities such as Employment Development Department,
- Funding SOC and audit services allowing more entities to invest in localized security improvements,
- Providing over 50 policy/standard templates adopted by departments.

Additional support is required for centralized security services to be offered out of CDT to help departments outsource technical security protection measures, to increase capacity and enable entities to focus inward on administrative security processes. Cal-Secure outlines the current services offered by the State which improve entities, as well as a roadmap of additional capabilities needed to be supported going forward.

a. CDT does not adequately follow up to ensure Entities' timely compliance with self-reporting requirements:

Elaine Howle
December 17, 2021
Page 6 of 8

⑭ CDT does not concur with this observation. CDT conducts comprehensive pre and post-audit workshops to assist entities in the preparation for, and remediation of findings following their audits. Additionally, during post-audits CDT conducts a comprehensive review of deficiencies and outstanding POAMs items. CDT also follows up at the Agency level to ensure compliance by state entities.

CDT dedicates efforts to track the completion of self-reporting, and report on trends that require improvement across multiple reporting entities. Beginning July 2022 CDT will present identified trends that require improvement across multiple reporting entities at the individual Agency dashboard review meetings and standing Information Technology Council (ITEC) and Information Security Advisory Council (ISAC) Governance meetings so that ITEC and ISAC membership may reinforce use of consolidated remediation efforts provided and or coordinated at the Agency and state levels where feasible.

b. CDT does not leverage reporting Entities responses to the Nationwide Review to help them improve their Information Security:

⑧ This particular finding is purely CSA's opinion and is not related any particular performance criteria that CDT's needs to comply pursuant to statute or policy.

⑨ As described above, NCSR scores are not objective basis for evaluating an entity's cybersecurity maturity. While this is a pertinent observation that CDT will take into consideration for future audits.

c. CDT failed to complete timely updates to the Information Security Standards with which reporting Entities must comply:

⑮ This particular finding is purely CSA's opinion and is not related any particular performance criteria that CDT's needs to comply with pursuant to statute or policy.

While CDT has generally adopted NIST 800-53 is a minimum standard for the state entities, SAM 5300 clearly states that the state has implemented additional standards. Pursuant to SAM 5300 - Entities shall ensure their security control selections and tailoring, at a minimum, comply with the State-defined Security Parameters for NIST SP 800-53 (SIMM 5300-A) and the prioritization of their information security program development and implementation align with the Foundational Framework for Information Security (SIMM 5300-B). Further, SIMM 5300-A is mapped to specific NIST 800-53 controls.

⑯ State entities seeking guidance on the appropriate security controls are directed to NIST 800-53 rev for the latest updates.

The pandemic response efforts shifted everyone's focus, to ensure government operations is conducted in a secure and privacy enabled manner. During the pandemic CDT incorporated Statewide Information Management Manual (SIMM) updates to provide focused guidance to combat immediate threats. CDT has released a number of SIMMs within 3-year audit cycle that are pertinent and up-to-date e.g. cloud security standard (SIMM 5315-B), end point protection standard (SIMM 5355-A), vulnerability management standard (SIMM 5345-A), phishing exercise standard (SIMM 5325-A). In addition, CDT has posted updated maturity metrics (SIMM 5300-C).

The pandemic response efforts shifted everyone's focus, to ensure government operations is conducted in a secure and privacy enabled manner. During the pandemic CDT incorporated Statewide Information Management Manual (SIMM) updates to provide focused guidance to combat immediate threats.

5. The recent increase in Telework has created new Information Security Risks for reporting Entities that CDT must continue to address:

This particular finding is purely CSA's opinion and is not related any particular performance criteria that CDT's needs to comply with pursuant to statute or policy. (17)

CDT in collaboration with CMD completed 92 RACE assessments against state entities to ensure they are adequately prepared and detect vulnerabilities in their IT infrastructure as they quickly transitioned to telework. CDT has and will continue to monitor the threat landscape and review NIST 800-53 updates and appropriately updated policy and guidance to state entities.

Please contact Kirk Marston at 916-208-6896, if you have questions.

Sincerely,

Vitaliy Panych

Vitaliy Panych,
State Chief Information Security Officer
California Department of Technology

cc: Yolanda Richardson, Secretary, Government Operations Agency
Amy Tong, Director, California Department of Technology
Russ Nichols, Chief Deputy Director, California Department of Technology

Blank page inserted for reproduction purposes only.

COMMENTS

CALIFORNIA STATE AUDITOR'S COMMENTS ON THE RESPONSE FROM THE CALIFORNIA DEPARTMENT OF TECHNOLOGY

To provide clarity and perspective, we are commenting on CDT's response to our audit. The numbers below correspond to the numbers we placed in the margin of CDT's response.

① Although CDT claims in its response that compliance audits were re-prioritized during the pandemic, CDT did not provide us with evidence of it postponing any audits for this reason. In fact, CDT's audit and assessment managers stated that, although CDT rescheduled a few audits for other reasons, no audits were rescheduled due to the pandemic.

② Our audit report accurately reflects the evidence and department perspective provided during the course of the audit. Although CDT states in its response that the number of high-risk entities identified for audits fluctuates, the state chief asserted during the audit that CDT plans to keep the same capacity of conducting 13 audits per year, which equates to 52 audits every four years.

③ Although CDT states in its response that it is projecting to complete 48 audits over the four-year cycle, this does not change the fact that CDT had completed only 31 of 39 audits it set out to complete by the end of the third year. Further, to complete a total 48 audits, CDT would have to finish 17 audits in the final year of its four-year oversight life cycle. While this is a laudable goal, we note that CDT only completed an average of 10 audits per year over the first three years of the oversight life cycle.

④ CDT asserts in its response that it does not plan to audit all entities. However, during the audit, the security risk governance manager stated that CDT intends to calculate a maturity metric score for each of the 108 reporting entities, which it cannot do unless it audits the entities. Further, as we discuss on page 20, the state chief indicated that CDT has little confidence in self-reported information and that it prefers to use independently verified information. By choosing to not audit all reporting entities, while also not utilizing self-reported information, it is not apparent how CDT will ever have a clear picture of the overall status of the State's information security.

⑤ CDT does not clearly state what it believes is misleading about Figure 2. Nevertheless, Figure 2 accurately describes CDT's oversight process.

⑥ Our audit report is not misleading; rather, it includes highly relevant facts that CDT neglects to address in its response. As we state on page 18, although CDT adopted the maturity metrics scoring methodology in March 2018, it had yet to revise its audit program to reflect the new criteria for privacy controls when it began its four-year oversight life cycle in July 2018. Thus, the criteria for the maturity metrics changed before the audits started and CDT had the opportunity to revise its audit methodology prior to beginning these audits, but it did not do so. As a result, CDT did not assess the entities on all required criteria and was not able to calculate maturity metric scores for nine of the 31 entities it audited.

⑦ We discussed the proposed IT project because the state chief pointed to the project as a solution that would allow CDT to more efficiently conduct its audits. However, as CDT states in its response, the IT project does not yet exist. Further, as we state on page 18, implementing a new IT project can take years. Therefore, CDT is taking a great risk by maintaining the status quo and waiting so long to determine what types of information security deficiencies may exist across the State.

⑧ Contrary to CDT's statement that the finding is purely our opinion, it is a fact that CDT does not leverage information from the nationwide review. As we state on page 20, the manager of CDT's security risk governance unit stated that CDT does not place much value on the nationwide review and therefore does not aggregate the information to identify statewide trends. However, CDT is missing an opportunity to use these results to identify the most common information security deficiencies across the State and provide targeted guidance to help entities remediate their deficiencies. Further, it should not take a specific requirement in statute to prompt CDT to leverage readily available information to help it fulfill its statutory purpose, which includes ensuring the confidentiality, integrity, and availability of state systems.

⑨ On page 20, we acknowledge CDT's concern that some entities may understate their information security in hopes of securing more federal grant funding. However, we found this concern to be unfounded. As we discuss on page 21, entities performed worse on CDT's maturity metrics than what they self-reported on the nationwide review. While we agree that independently verified information is preferable to self-reported information, CDT has been slow to complete its compliance audits and the nationwide review could help it develop a clearer picture of the status of the State's information security.

⑩ As we state on page 20, entities' scores on the nationwide review have remained stagnant over the past three years and CDT has not used the information about common deficiencies identified during the review to help the entities improve their information security. Although we agree that independently verified information is preferable to self-reported information, CDT's failure to sufficiently implement its compliance audits has left the State without a clear picture of the status of its information security. CDT should use the nationwide review scores to help focus that picture.

⑪ CDT's response suggests that entities can improve their information security without seeing their maturity metric scores increase. However, as we state on page 9, CDT designed the maturity metrics to be consistent so that it can measure each entity's progress and compare information security development across entities. Therefore, entities' maturity metric scores should increase as they improve their information security; that is the point of creating such a metric. Although three entities saw their maturity metric scores increase, as we discuss beginning on page 21, the majority of entities that received multiple scores saw their scores decrease, indicating a lack of progress in improving their information security.

⑫ Our statement regarding what CDT shared with the Legislature is accurate. As we state on page 23, we reviewed CDT's legislative briefing presentations and found that it generally did not share detailed information about the nationwide review or the maturity metric scores it has calculated. In fact, CDT was only able to provide evidence of one instance in which it shared information regarding maturity metric scores with the Legislature.

⑬ Although CDT lists various activities it has undertaken to help reporting entities improve their information security, available information—such as the maturity metrics and independent security assessments—show that reporting entities continue to perform poorly. As we discuss beginning on page 21, the majority of entities that received multiple maturity metric scores saw their scores decrease, indicating a lack of progress in improving their information security. Further, as we state on page 22, we analyzed 135 independent security assessments completed between January 2018 and March 2021 and found that the State's progress remained relatively flat. Specifically, the State's average score was 52 during the first year before increasing slightly during the middle two years, only to drop back down to a score of 52 within the first three months of the final year.

⑭ CDT's response misses the point of our concern. CDT's response focuses on audit-related activities, such as pre- and post-audit workshops. However, these activities do not address its failure to ensure entities' timely compliance with self-reporting requirements, which are separate from audits. For example, as we state on page 24, reporting entities had completed self-assessments for only 172 of their nearly 3,300 critical IT systems; pre- and post-audit workshops do not directly address these deficiencies.

⑮ Contrary to CDT's assertion that the finding is purely our opinion, it is a fact that CDT did not fulfill its statutory responsibility to update the State's information security standards. As we state on page 26, the federal government released a draft copy of a NIST 800-53 revision in August 2017 and CDT used this draft in developing the methodology it published in March 2018 for calculating maturity metric scores. However, CDT did not hire someone to assist with updating the State's policies until nearly a year after the federal government published the official updates in September 2020.

⑯ As we state on page 26, both SAM 5300 and SIMM, which CDT is required to update, continue to direct reporting entities to an outdated version of the federal information security standards.

⑰ CDT's objection to our finding is ambiguous. On page 28, we state that CDT's guidance regarding steps employees should take to secure their personal devices used for telework is unclear. When we followed up with CDT regarding this matter, it stated that it plans to update the language to make it clearer. Maintaining information security policies, procedures, and standards is a statutory requirement for CDT.