GAVIN NEWSOM
GOVERNOR

NANCY WARD
DIRECTOR

August 7, 2025

The Honorable Jesse Gabriel
Chair, Assembly Committee on Budget
1021 O Street, Suite 8230
Sacramento, CA 95814

The Honorable Scott Wiener
Chair, Senate Committee on Budget
1021 O Street, Suite 8620
Sacramento, CA 95814

Gabriel Patek, Legislative Analyst
Legislative Analyst's Office
925 L Street, Suite 100
Sacramento, CA 95814

Subject: Report to the California Legislature on the Summary of Progress on Cal-Secure Multi-Year Horizon Roadmap as Required by SB 104, Provision 4

Dear Assemblymember Gabriel, Senator Wiener, and Mr. Patek:

Please find the closed "Report to the California Legislature on the Summary of Progress on Cal-Secure Multi-Year Horizon Roadmap" pursuant to Budget Act of 2023, 0690-001-0001, Provision 4 (Senate Bill 104, Chapter 189, Statutes of 2023). This report is to be submitted to the chairpersons of both budget committees of both houses of the Legislature and the Legislative Analyst's Office.

If you have any questions, please contact the Office of Legislative and Governmental Affairs, Deputy Director Yvonne Dorantes at (916)364-4525 or Yvonne.Dorantes@CalOES.ca.gov.

Sincerely,

Nancy Ward

NANCY WARD
Director

Enclosure:
Report to the California Legislature on the Summary of Progress on Cal-Secure Multi-Year Horizon Roadmap

3650 SCHRIEVER AVENUE, MATHER, CA 95655
(916) 845-8506 TELEPHONE (916) 845-8511 FAX
www.CalOES.ca.gov

REPORT TO CALIFORNIA LEGISLATURE
REGARDING THE STATUS OF CAL-SECURE PROGRESS REQUIRED BY THE BUDGET ACT OF 2023

SUMMARY OF PROGRESS ON THE CAL-SECURE MULTI-YEAR HORIZON ROADMAP

FEBRUARY 1, 2025

Table of Contents

Executive Summary 3
Background 4
Cal-Secure Progress 6
Cal-Secure Technical Capability and Constraints 6
Baseline Security Controls 6
Technical Capability Priority 1 Progress 7
Technical Capability Priority 2 Progress 8
Technical Capability Priority 3 Progress 9
Technical Capability Priority 4 Progress 10
Technical Capability Priority 5 Progress 11
Technical Capability Constraints 12
Cal-Secure Maturity 13
Independent Security Assessment 14
ISA Constraints 17
California Cybersecurity Maturity Metrics 18
Nationwide Cybersecurity Review 21
Cal-Secure Key Community-Driven Initiatives & Constraints 23
Key Initiative Priority 1 Progress 24
Key Initiative Priority 2 Progress 25
Key Initiative Priority 3 Progress 26
Key Initiatives Priority 4 Progress 27
Key Initiatives Priority 5 Progress 28
Key Initiatives Constraints 29
Funding & Positions 30
Conclusion 32
Glossaries 33
Cal-Secure Roadmap Glossary 33
Independent Security Assessment Glossary 39
California Cybersecurity Maturity Metric Glossary 46

CONFIDENTIAL

Appendix A: ISA Criteria & Cal-Secure Roadmap Mappings 48
Appendix B: NCSR Criteria & Cal-Secure Roadmap Mapping 50
Appendix C: Cal-Secure Technical Capability Completion Score Definitions..... 52

CONFIDENTIAL

Executive Summary

Pursuant to the Budget Act of 2023, 0690-001-0001, Provision 4 (Senate Bill 104, Chapter 189, Statutes of 2023), the Office of Emergency Services (Cal OES), in consultation with other California Cybersecurity Integration Center (Cal-CSIC) partners, shall develop a report on the state implementation of cybersecurity initiatives and technical capability investments in Cal-Secure. The report includes the following:

a) A summary of state entities' implementation of the cybersecurity initiatives and technical capability investments in Cal-Secure, including, but not limited to, each state entity's progress through Cal-Secure's multi-year horizon roadmap;

b) A list of the initial outcomes from additional funding and positions provided to state entities in 2023/24 to implement Cal-Secure, such as demonstrated improvements in entities' cybersecurity maturity based on audits performed by the California Department of Technology (CDT); and

c) Clear progress towards remediation of capability gaps identified by the Cal-CSIC in its analysis of Cal-Secure progress.

Moreover, cybersecurity maturity information has been summarized and reviewed by the Chief Information Security Officer (CISO) and the Cal-CSIC due to confidentiality, to ensure no sensitive cybersecurity vulnerability information is unnecessarily exposed. Where requested information is not provided by reporting agencies to the Cal-CSIC, the Cal-CISC will specify in this report.

Overall, this report aims to provide a broad view of the state's cybersecurity maturity, and insights into the ongoing progress in implementing technologies to meet the technical capabilities and key initiatives outlined in the Cal-Secure roadmap. Specifically, this report focuses on the Government Code Section 11546.1 entities which include state agencies and organizations within the executive branch that are under the direct authority of the governor. Data points enumerated in this report are derived from Cyber Security Policy Audits, Independent Security Assessments (ISA), self-attestation surveys, and compliance documentation obtained by CDT.

As Cal-Secure begins its fourth year, the state is well over halfway to implementing technical capabilities. Moreover, the state continues to make improvements in each year, moving closer to and exceeding the 80 percent implementation baseline set by the state CISO. California agencies and entities continue to take Cal-Secure technical capabilities and key initiatives seriously, implementing "optional" tasks to strengthen their respective cybersecurity landscapes. Despite this progress, government entities remain prime targets for cyberattacks due to the sensitive data they manage. As a state of nearly 40 million people and the fifth largest economy, worldwide, California is not exempt from cyberattacks. During the development and review of this report, CDT and the Cal-CSIC determined sensitive cybersecurity vulnerability

CONFIDENTIAL

information may be unnecessarily exposed. With this understanding, the Cal-CSIC and the CDT chose to omit a breakdown of each state entity's progress through the Cal-Secure multi-year horizon roadmap. Despite entity specific data, this report accurately details Cal-Secure's comprehensive approach, successes, and shortfalls, leaving room for continued improvement and progress.

Background

Digital innovation provides a path forward as California advances our commitment to a "California for All". As cybersecurity threats evolve, California state government remains dedicated to protecting the privacy and security of all Californians' information. To be accountable to this commitment, we must prepare for cyberattacks of any scale. The California Homeland Security Strategy and the State Technology Strategic Plan: Vision 2023, made it clear that a collaborative approach was needed to identify, manage, and mitigate cybersecurity risks. It is critical that California continues to prioritize its resources to manage the most significant cyber risks and safeguard the services for the residents that depend on them. To address these challenges, the Newsom Administration developed Cal-Secure, a multi-year cybersecurity roadmap for California. Designed to be flexible and innovative, Cal-Secure enables the state to manage existing and future threats more effectively. Furthermore, Cal-Secure defines a path for state entities to strengthen their cybersecurity measures so that they may continue to provide critical services without interruption.

The Cal-Secure roadmap was created through a collaborative process with the Cal-CSIC and its core four partners, Cal OES, California Highway Patrol (CHP), CDT, and California Military Department (CMD). The roadmap is intended to outline a prioritized set of capabilities the state must adopt as a phased approach. The roadmap was announced in October 2021 as an overarching framework to help state entities incrementally improve their cyber resilience and maturity over time.

The roadmap is organized into two categories, required technical capabilities and community-driven initiatives. The roadmap spans five phases, and in each phase, priorities are grouped by technical controls and key initiatives that entities must focus on. Each priority group was determined by balancing the complexity of implementation with the potential for significant security control improvements. While the roadmap provides a standard priority across technical capabilities and key initiatives, agencies may emphasize different areas of cybersecurity based on their specific needs, regulatory environments, and risk profiles. In turn, some agencies may prioritize certain capabilities sooner than others, depending on the criticality of their mission. It is possible some of these priorities may diverge from the general outline provided in the Cal-Secure roadmap.

CONFIDENTIAL

Technical capabilities are a baseline snapshot of where security exists at a foundational level, ensuring that the organization has some level of protection. However, technical capabilities need to be thoroughly implemented, requiring growth and development for a comprehensive implementation across the organization. Therefore, routine audits and assessments guide entities toward a more compressive implementation of their technical capabilities.

The Cal-Secure roadmap outlines 29 technical capabilities organized into fiscal year (FY) priorities. Each priority has a group of technical controls entities should seek to implement over the five-year Cal-Secure Horizon roadmap. These are detailed in the table below.

Priority 1 FY 21/22	**Priority 2** FY 22/23	**Priority 3** FY 23/24	**Priority 4** FY 24/25	**Priority 5** FY 25/26
• Anti-Malware Protection • Anti-Phishing Program • Multi-Factor Authentication • Continuous Vulnerability Management	• Asset Management • Incident Response • Continuous Patch Management • Privileged Access Management • Security and Privacy Awareness Training • Security Continuous Monitoring 24/7/365 • Cloud Security Monitoring	• Data Loss Prevention • Log Management • Network Threat Detection • Network Threat Protection • Threat Intelligence Platform • Application Security • Operational Technology Security	• Disaster Recovery • Enterprise Sign On • Mobile Device Management • Application Development Security • Application Whitelisting • Software Supply Chain Management	• Identity Lifecycle Management • Insider Threat Detection • Network Access Control • Enterprise Encryption • Mobile Threat Defense

The respective California state agencies and entities drive the execution of Cal-Secure key initiatives, reflecting a shift toward proactive and collective responsibility rather than mandated compliance. These initiatives focus on building a culture of security awareness and best practices. This culture shift encourages innovation and continuous improvement in security, representing the direction the cybersecurity community needs to move toward.

CONFIDENTIAL

Cal-Secure Progress

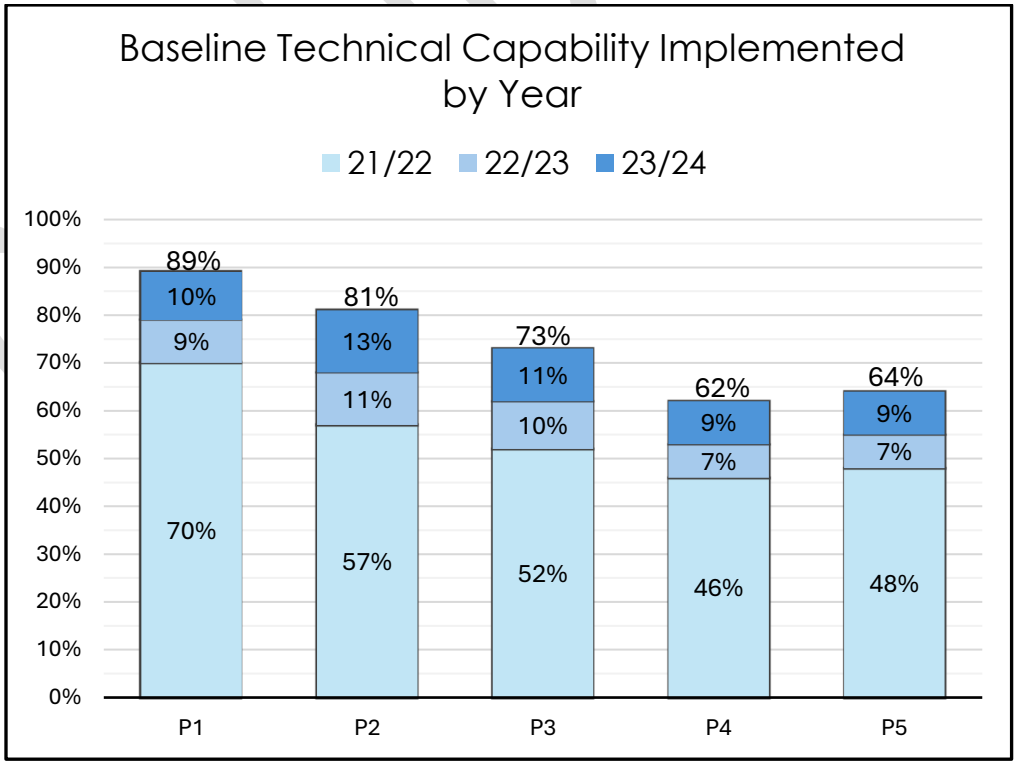
The Cal-Secure roadmap is now entering its fourth year and Technical Capability Priority 4. Audits and assessments are conducted in two-year intervals to address gaps in security controls and to determine the growth of each entity's technical capabilities. During these intervals, it is assumed that each entity's baseline operating capabilities remain constant. When smaller entities such as boards, commissions, and conservancies are incorporated within a parent entity, they adopt the parent entity's scores and capabilities.

The state's goal, set by the CISO, is to achieve a minimum baseline of 80 percent completion for each state agency of all technical capabilities implemented. However, there is an optimal target of 90 percent to enhance preparedness against future cyber threats. This report provides further details on the maturity of these capabilities.

Cal-Secure Technical Capability and Constraints

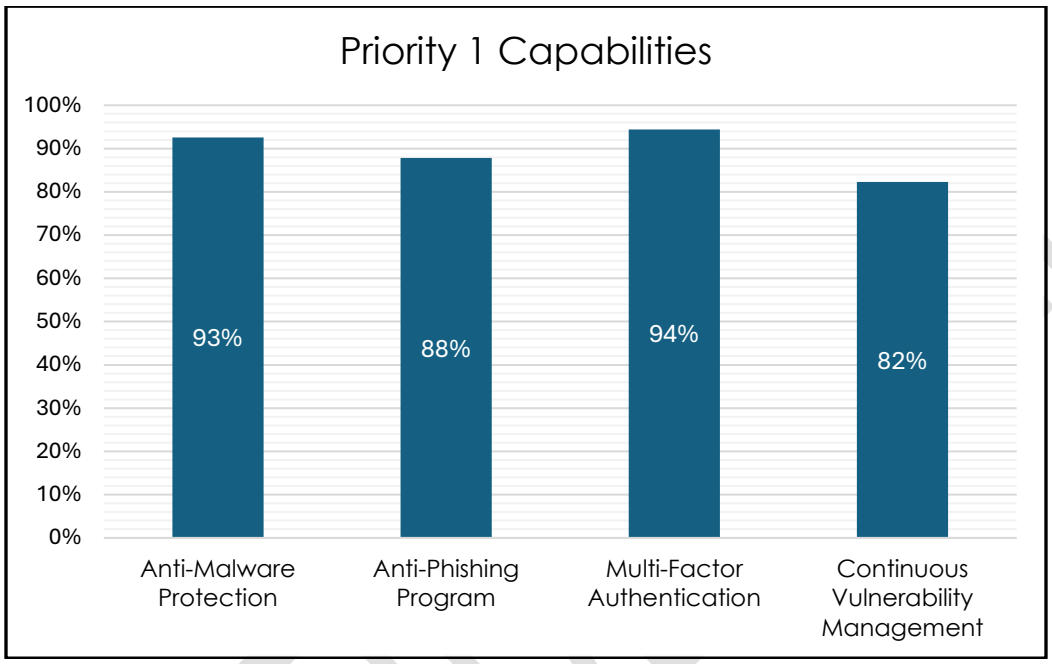
Baseline Security Controls

The chart below illustrates the average progress of baseline security controls implemented by state entities and agencies. This demonstrates the progress towards implementing the 29 controls by each fiscal year to create a baseline security posture. The chart below aggregates all Government Code 11546.1 entities progress to calculate the overall state average, excluding non-CDT reporting entities, which are defined under Gov. Code 11000.



Technical Capability Priority 1 Progress

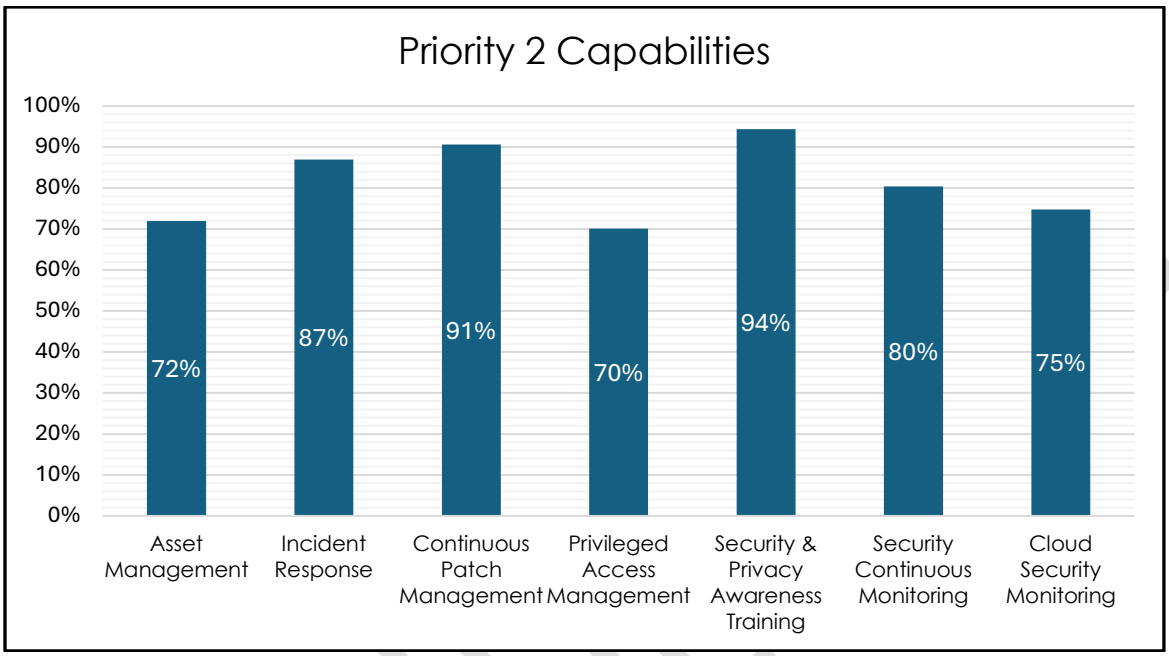
The following chart breaks down the technical controls in Priority 1, set for FY 2021/22. An average of 89 percent of all Priority 1 capabilities have been implemented by agencies by the end of the reporting period. This exceeds the minimum baseline rate of 80 percent and almost meets the 90 percent optimized goal set by the state CISO.



Generally, more entities need to implement Continuous Vulnerability Management to increase the state's average. While each capability has achieved the 80 percent baseline target established by the CISO, CDT recommends that departments continue to prioritize and advance their maturity in vulnerability management to maintain and enhance their security posture. As a stopgap, CDT, in partnership with Cal-CSIC, implemented statewide capabilities to support state entities, including vulnerability disclosure and external attack surface management programs.

Technical Capability Priority 2 Progress

The following chart below breaks down the technical controls in Priority 2, set for FY 2022/23. An average of 81 percent of all Priority 2 capabilities have been implemented by agencies by the end of the reporting period. This indicates that the state has a strong level of implementation in these capabilities.

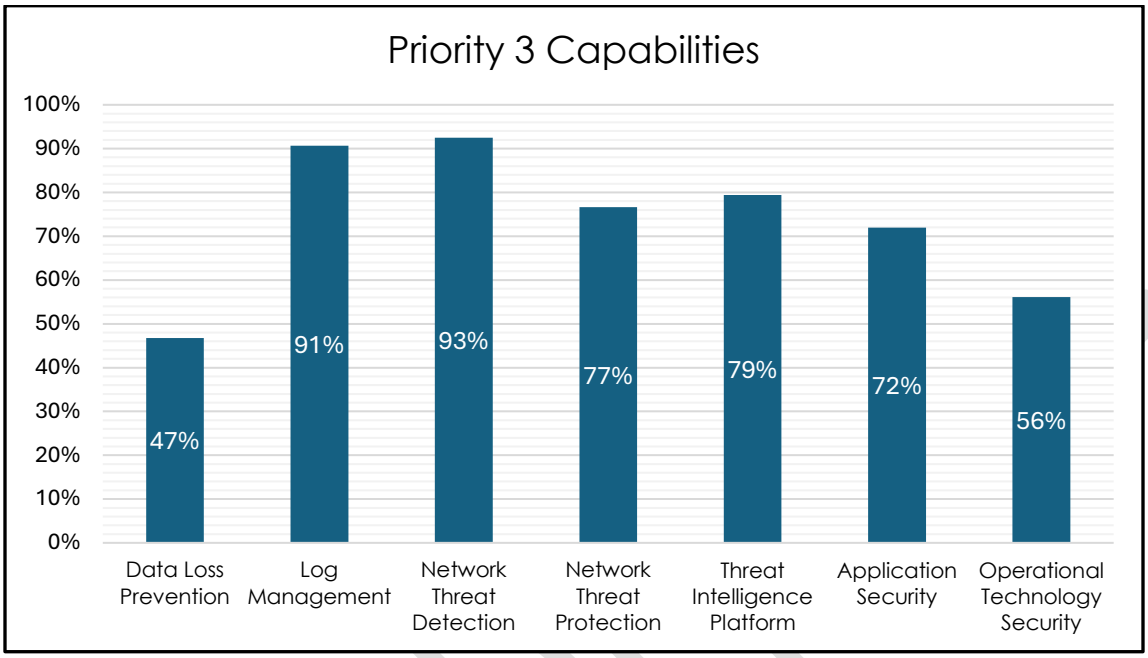


The state's average in asset management, privileged access management, and cloud security are below the 80 percent baseline goal set by the state CISO and should remain a focus for entities. As a provisional measure, CDT implemented a cloud-smart policy which requires new cloud environments to implement cloud security monitoring as part of their design. All state entities and agencies that are new and existing cloud customers are required to establish acceptable levels of continuous security monitoring or be enrolled in the State Security Operations Center as a Service (SOCaaS) for their continuous security monitoring.

With increases in data breaches, insider threats, and accidental misuse, CDT is currently developing standards for zero trust architecture and server hardening. These standards will offer guidance and requirements to address gaps in privileged access management (PAM) and asset management, resulting in strengthened security controls in these domains.

Technical Capability Priority 3 Progress

The chart below details the technical controls in Priority 3, set for FY 2023/2024. An average of 74 percent of all Priority 3 technical capabilities have been implemented by agencies.



CDT has determined that more improvements are needed by entities in data loss prevention, application security, and operational technology security. Currently, CDT has a few interim measures to monitor for weaknesses in these areas.

For data loss prevention, CDT requires departments to utilize the California Government Enterprise Network (CGEN) as their primary source for internet access, unless an exemption is approved. CGEN consists of a vendor-managed network that includes wide area connectivity, flexible routing, domain name resolution, packet monitoring, secure connections, and other network services. These services enable connections to statewide services by linking customers to CDT headquarters, hosting facilities, the internet, other state agencies, counties, and external business partners. By using CGEN, cleartext data can be monitored against data prevention loss policies, enhancing overall security, and protecting sensitive information.

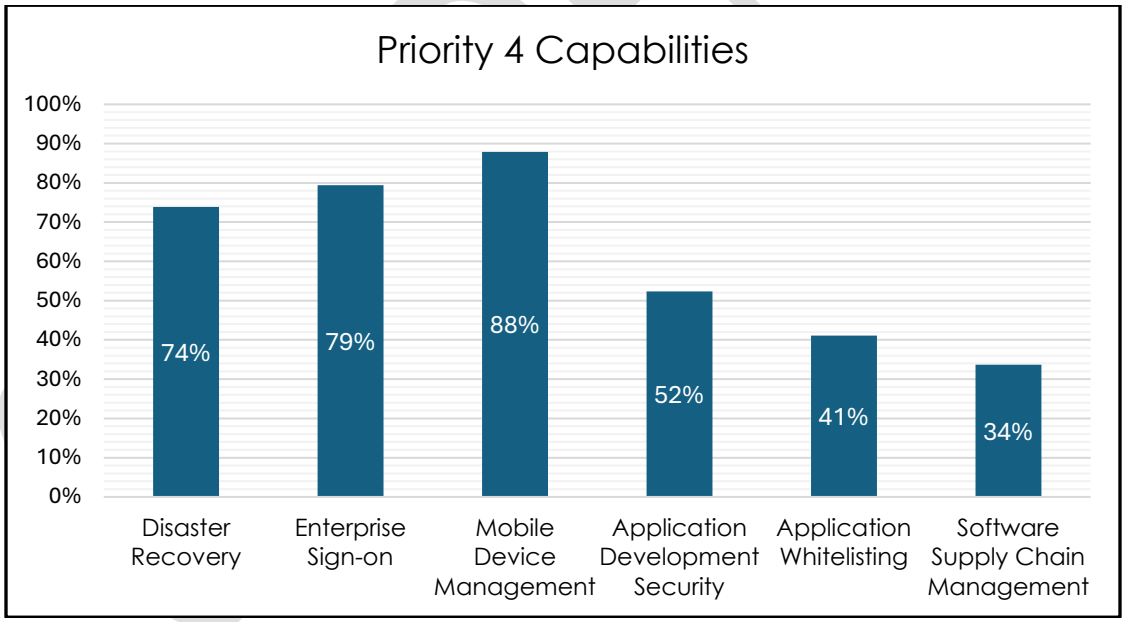
For application security, CDT is providing guidance based on federal frameworks that highlight best practices for securing the application lifecycle. This is based on the National Institute of Standards and Technology (NIST) Risk Management Framework (NIST RMF 800-37). This extends to application providers within the procurement and acquisition terms and conditions.

Priority 3 has a focus on the technical capability of Operational Technology (OT) security. Broadly, OT security is the practice of protecting the hardware and

software systems that monitor and control industrial control systems and equipment (e.g. dams, filtration systems, processing plants, etc.). As an example of the scale of OT operated by state government, drinking water systems alone account for 138 such systems. Drinking water systems operated by prisons, California Department of Transportation (Caltrans), California Department of Forestry and Fire Protection (CAL FIRE), California Department of Corrections and Rehabilitation (CDCR), California Department of Water Resources (DWR), and California State Parks include OT. CDT is actively working to encourage state entities to practice sound asset management techniques and to work with their respective engineering teams and to secure their OT. To support OT security efforts and growth, the Cal-CSIC and CDT are operationalizing an OT lab. This lab will be used as a testing and training environment containing OT critical infrastructure, which will extend to both state and local entities.

Technical Capability Priority 4 Progress

The following chart breaks down the technical controls in Priority 4, set for FY 2024/25. Although the state is currently in the middle of the fiscal year, and Priority 4, an average of 61 percent of the technical capabilities have already been implemented by agencies at the time of this report.

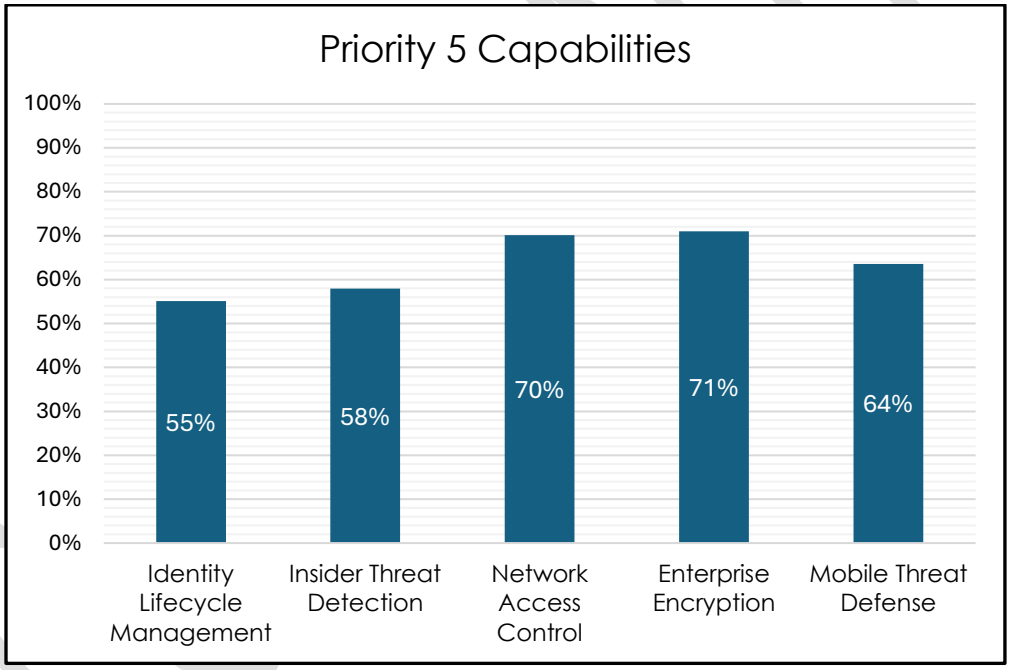


As a preliminary approach, CDT is collaborating and registering interested entities in an external vulnerability scanning tool, provided by CDT free of charge, to monitor supply chain risk. This tool provides insights into public-facing servers managed by departments and includes information on commonly used vendors, allowing entities to better understand the inherited risks in their supply chains. Greater adoption of this tool is expected to enhance supply chain management practices.

Additionally, CDT conducts annual Technology Recovery Plan (TRP) reviews for agencies. TRP reviews are comprehensive evaluations designed to identify gaps in an entity's recovery plans and overall security posture. Based on the findings from these reviews, CDT offers tailored recommendations aimed at strengthening the entities' recovery strategies. This proactive approach ensures that the entities are better prepared to mitigate risks and respond effectively to potential threats, ultimately enhancing their resilience and disaster recovery capability.

Technical Capability Priority 5 Progress

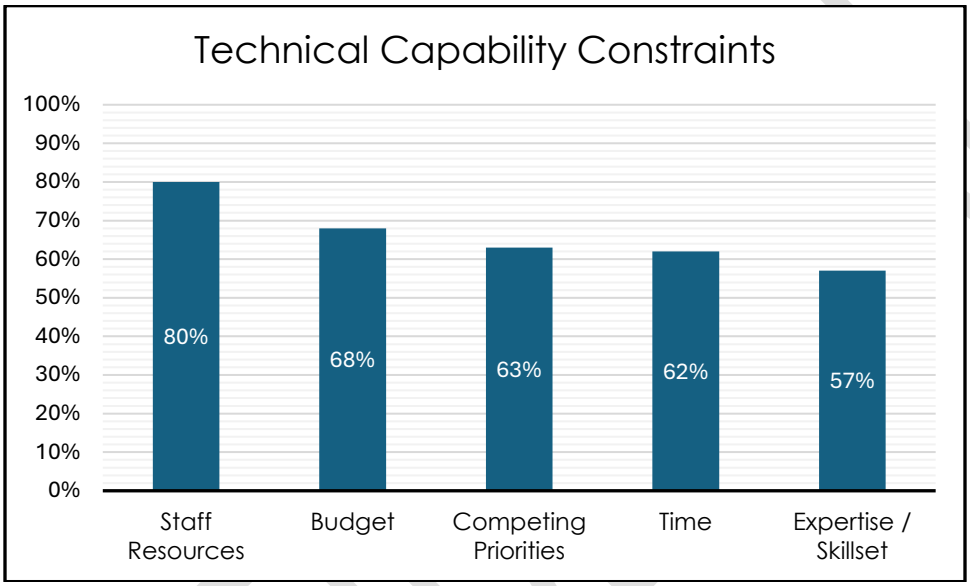
The chart below details the technical controls in Priority 5, which are targeted for FY 2025/26. Agencies have already begun implementing these controls, with an average completion rate of 64 percent by the end of the reporting period. Current completion levels reflect varying levels of maturity across these technical capabilities.



As a mitigation effort, CDT is updating audit and ISA criteria to address gaps in the Priority 5 technical capabilities. The revised criteria will introduce additional checks in the aforementioned areas with any identified gaps being recorded in the entity's risk register. This will increase visibility into areas needing improvement and help drive the adoption of measures to close those gaps. Moreover, CDT is enhancing guidance on encryption by updating cybersecurity standards. As existing standards are updated, a key focus will be on internal encryption controls, aiming to promote greater adoption towards enterprise encryption.

Technical Capability Constraints

The chart below highlights the primary constraints identified by departments. Since departments could report multiple constraints, the chart reflects various constraint areas. Across all surveyed agencies and entities, these constraint areas were cited as significant barriers to implementing technical controls. While this information was primarily sourced from a survey of state agencies conducted by OIS, though similar constraints are also highlighted in the risk registers submitted by these entities.



Agencies report that insufficient staffing and funding remain the most significant challenges in implementing initial operating capabilities. Additionally, time and competing priorities are notable constraints, suggesting that organizational focus is often diverted away from cybersecurity implementation efforts.

The following chart correlates California's average security staffing [Personnel-Years (PY)] in respect to an entity's size and Cal-Secure score.

Entity Size Thresholds	Average Num. of (PY)/ Entity Size	Dedicated Security (PY)	Sec/Staff Ratio	Industry Recommend Security PY	Cal-Secure Score
Very Small 0-49	17	0.24	1.41%	1	78%
Small 50-600	223	3.5	1.57%	3-10	76%
Medium 601-1999	896	6.5	0.73%	10-20	77%
Large 2000 - 10,000	5,018	10.5	0.21%	20-50	81%
Very Large 10,001+	30,703	23.5	.08%	50-200+	85%

Despite the security-to-staff ratio decreases, marginal increases in security staff size, regardless of the entity's size, lead to significant improvements in the implementation of Cal-Secure technical capabilities. Overall, this is reflected in the Cal-Secure score average.

Cal-Secure Maturity

Organizational maturity can be used to measure Cal-Secure progress and evaluated in several ways (or models):

- Independent Security Assessment (ISA)
- California Cybersecurity Maturity Metrics (CCMM)
- Nationwide Cybersecurity Review (NCSR)

Maturity Model	Required By	Developed & Owned By	Assessment Performed By	Standards & Frameworks Used	Costs Covered By
ISA	Gov. Code Section 11549.3	California Military Department	California Military Department	Cal-Secure NIST SP 800-53[1] FIPS 199, 200[2]	Subject Entity
CCMM	Gov. Code Section 11549.3	CDT OIS	CDT OIS	SIMM/SAM[3]	CDT
NCSR	Federal grant programs	CISA[4], MS-ISAC[5], CIS	Entity self-assessment	NIST CSF[6], NIST SP 800-53[1], COBIT[7], CIS Controls[8], & HIPAA[9] (where applicable)	Federal Government

1. National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations, and its successor publications
2. Federal Information Processing Standards (FIPS) 199 Standards for Security Categorization of Federal Information and Information Systems, and its successor publications; FIPS 200 Minimum Security Requirements for Federal Information and Information Systems, and its successor publications.
3. Statewide Information Management Manual / State Administrative Manual
4. Cybersecurity and Infrastructure Security Agency
5. Multi-State Information Sharing and Analysis Center
6. NIST Cybersecurity Framework 2.0
7. Control Objectives for Information and Related Technologies: A framework for the governance and management of enterprise information and technology created by Information Systems Audit and Control Association (ISACA)Center for Internet Security
8. CIS Critical Security Controls (CIS Controls) are a prescriptive, prioritized, and simplified set of best practices that organizations can use to strengthen their cybersecurity posture.
9. Health Insurance Portability and Accountability Act

CONFIDENTIAL

Independent Security Assessment

The Independent Security Assessment (ISA) offers a third-party evaluation of an entity's deployed cybersecurity controls. The assessment criteria used within the ISA is set by CDT OIS. ISA participation is mandated every two years in accordance with Gov. Code Section 11549.3.

Among other functions, the ISA measures whether the Cal-Secure technical capabilities are adequately implemented throughout the organization, providing a more accurate reflection of the department's cybersecurity maturity. Entities that actively engage with the ISA team benefit from knowledge transfer and validation of their overall cybersecurity posture.

The Cal-Secure technical capabilities and the ISA criteria are mapped in Appendix A, serving as a reference to identify how each Cal-Secure technical capability is measured by the corresponding ISA criteria. The ISA tests for 39 control areas, which align with one or more of the 29 Cal-Secure technical capabilities. It should be noted that ISA criteria change over time to keep pace with rapidly evolving cybersecurity standards and requirements, so year-over-year comparisons can be difficult and should be considered carefully.

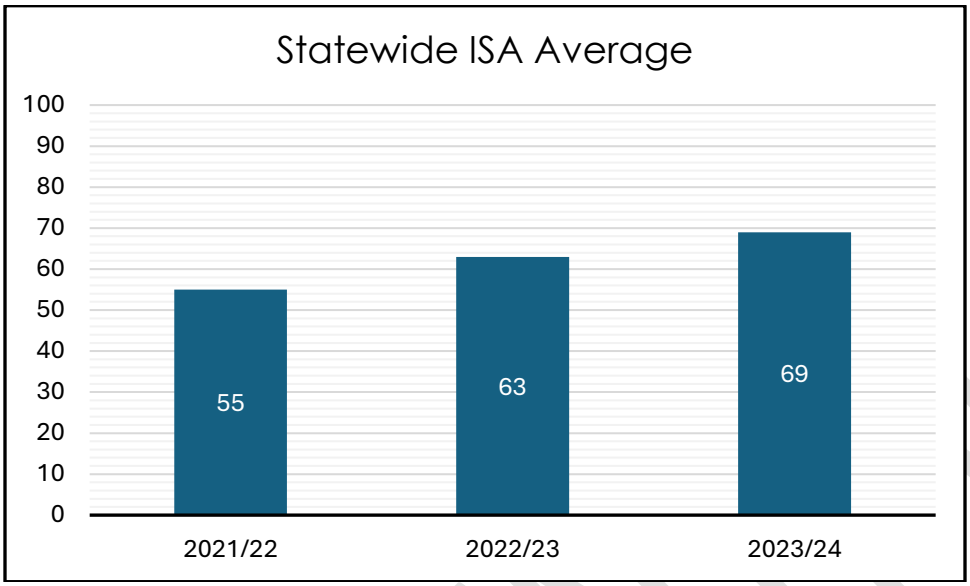
The CMD Cyber Network Defense Team conducts the ISA using a two-team approach. The risk analysis team conducts tasks related to defensive controls whereas, the penetration test team conducts activities related to offensive simulation operations. These two teams operate independently of each other and conduct operations at different intervals to validate if the Cal-Secure technical capabilities are comprehensively implemented.

Each technical capability requires entities to implement a series of associated security controls, which demand active and continuous improvement throughout their lifecycle and maturation. The ISA's objective is to assess the depth of maturity and effectiveness of each individual technical capability implemented. The state has established a minimum baseline, requiring each technical capability to achieve a 60 out of 100 while implemented.

To enhance assessment criteria and progressively raise maturity standards, CDT collaborates closely with Cal-CSIC and CMD. In turn, this allows the state to keep pace with the evolving cyber threat landscape.

CONFIDENTIAL

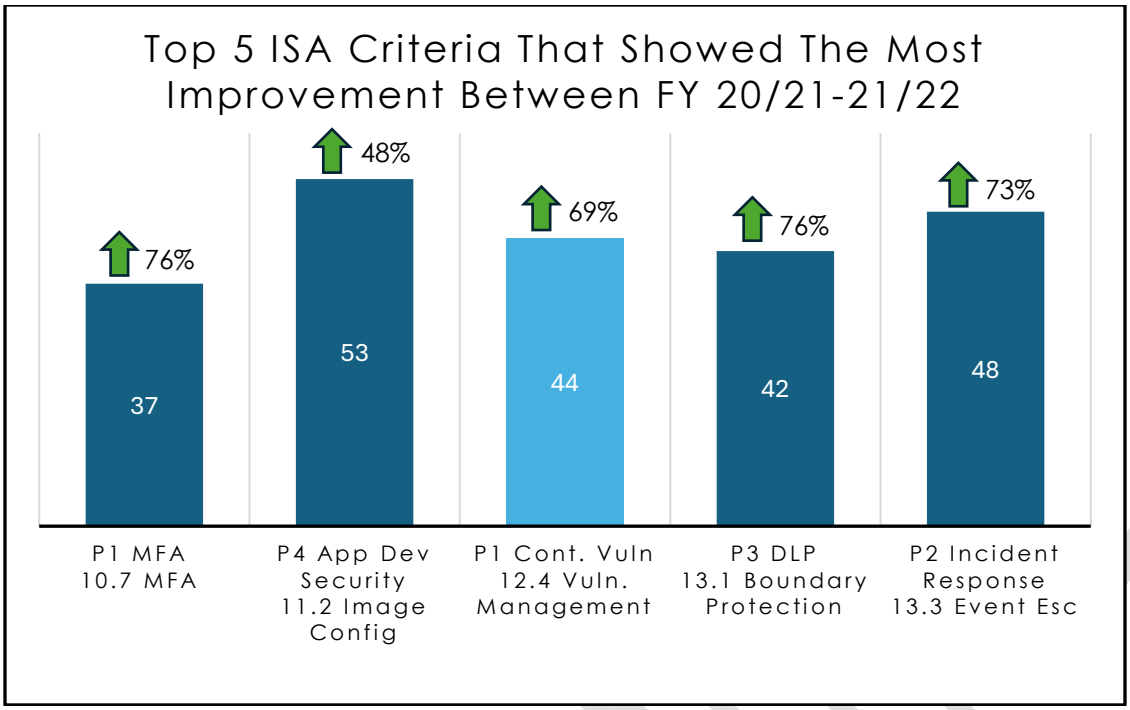
After an ISA is completed, a collective score is calculated to illustrate the current maturation and holistic state of the entity. The following chart breaks down the average ISA score of state entities over the last three fiscal years.



Throughout each fiscal year, various control areas improved. In FY 2021/22, the average ISA score for state agencies and entities was 55 out of 100. Entities had preliminary technical security controls in place, but still had significant gaps and deficiencies throughout their organization that were unaddressed.

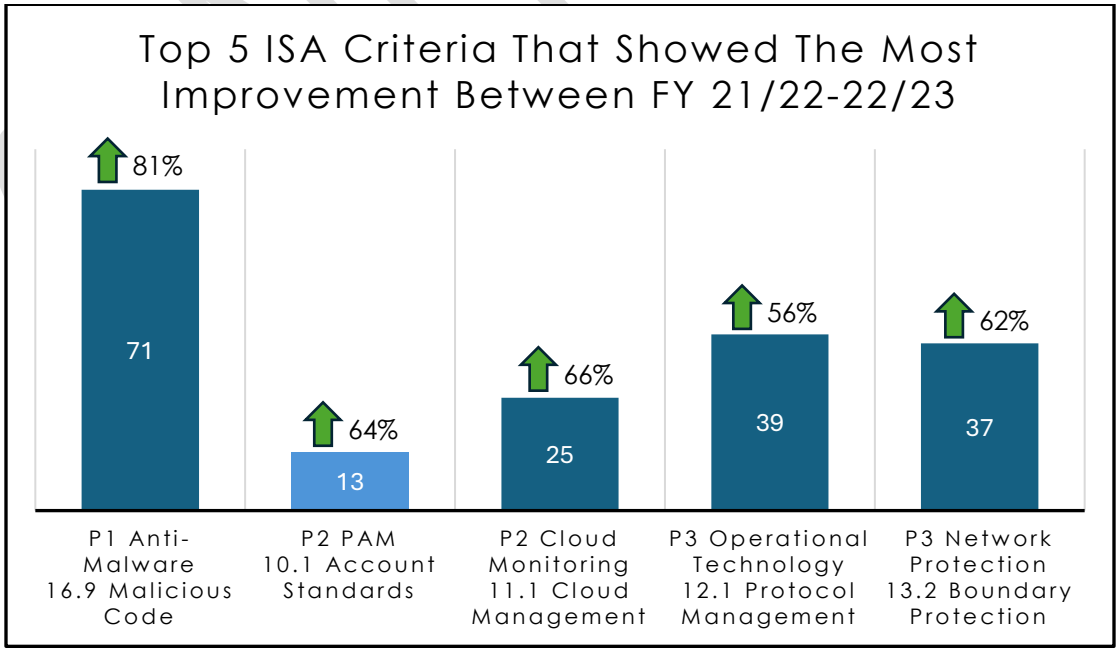
Of the 39 ISA criteria, the top five areas that improved between FY 2020/21 and FY 2021/22 in maturity were multifactor authentication, application development security, continuous vulnerability management, data loss protection, and incident response. The chart detailed below illustrates the average increase in technical capabilities during between FY 2020/21 to FY 2021/22.

CONFIDENTIAL



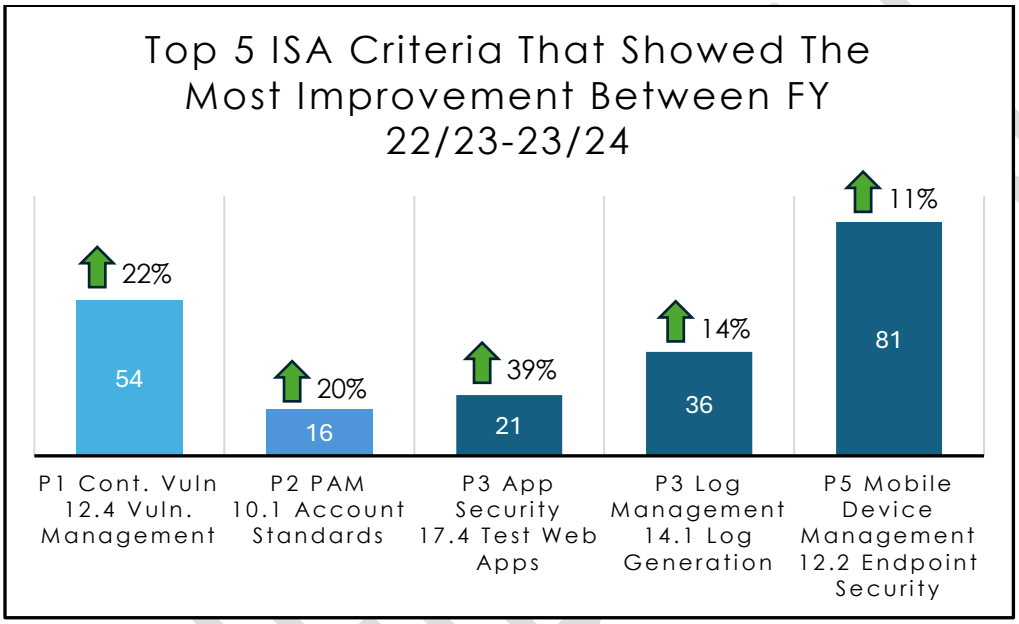
In FY 2022/23, the average score for state agencies and entities totaled 63 out of 100. This indicates progress by state entities in implementing foundational technical controls for cybersecurity. However, further efforts are needed by entities to advance beyond basic compliance.

The top five areas that improved between FY 2021/22 and FY 2022/23 in maturity were anti-malware protection, privileged access management, cloud security monitoring, OT security, and network threat protection.



In FY 2023/24 entities scored an average of 69 out of 100. As the upper limit of the 60 to 69 percent range, a score of 69 percent indicates that the state is nearing moderate maturity but has not yet reached full maturity. While the essential security mechanisms are in place, there are still opportunities to increase the depth of security practices to close remaining gaps.

The top five areas that improved between FY 2022/23 and FY 2023/24 in maturity were in the ISA areas of continuous vulnerability management, privileged access management, application security, log management, and mobile device management.



ISA Constraints

Smaller entities often score below state averages when managing security independently because they lack the ability to fund cybersecurity initiatives and struggle to fund their ISA. Currently, ISA costs range from $33,000 for an entity with 50 endpoints to $329,000 for an entity with 27,000 endpoints, at an average of $104,000 per ISA. This cost is generally always borne by the assessed entity in accordance with Gov. Code Section 11549.3. However, being integrated into a larger entity such as an agency allows them to benefit from the established cybersecurity maturity and resources if both entities agree upon terms of service. Otherwise, small entities lack sufficient funding for cybersecurity, which significantly reduces the state's overall score and requires outside help to improve their maturity scores.

California Cybersecurity Maturity Metrics

Cybersecurity audits (aka Information security policy audits or ISPAs) assess the maturity of each entity's policies and procedures, focusing on compliance and governance. As a result, the audit emphasizes policies and procedures over technical capabilities. Gov. Code Section 11549.3 authorizes CDT OIS to conduct an audit of Gov. Code Section 11546.1 entities' information security to ensure program compliance. Each entity is required to undergo an audit every two years, however, this requirement could also be satisfied with an ISA.

The audit process begins with an engagement letter sent to the entity's ISO and entity head six months prior to the audit. During this six-month period, the CDT Advisory Services Team provides the ISO with a list of required documents to demonstrate compliance with Statewide Information Management Manual (SIMM) and Statewide Administrative Manual (SAM) standards. As documents are submitted through the Secure Automated File Exchange (SAFE), a CDT-provided secure file transfer service, the CDT Audit Research Team reviews the materials and partially prepares the assessment. Field auditors then spend approximately three weeks onsite with the entity's ISO to collect any missing evidence or clarify unclear documentation. After finalizing the assessment, they compile the final audit report. An exit conference is held with the entity head and ISO staff to review findings. Based on identified gaps, a cybersecurity metrics maturity score is determined. Following the audit, the CDT Advisory Services Team continues working with the entity to address and resolve these gaps.

The CDT audit framework is based on NIST 800-53, Revision 5, which consists of 18 control families. These control families provide a foundation for establishing organizational guidelines and procedures to ensure a secure cybersecurity program. The CDT audit covers a range of policies and procedures from the following NIST control categories:

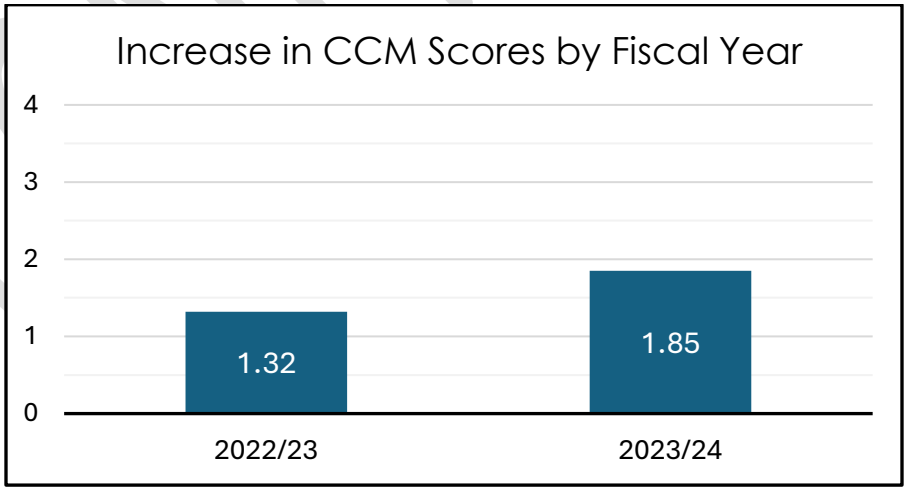
- Access Control
- Awareness & Training
- Audit & Accountability
- Security Assessment & Authorization
- Configuration Management
- Contingency Planning
- Identification & Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical & Environmental Protection
- Planning
- Personnel Security
- Risk Assessment
- System & Services Acquisition
- System & Communications Protection
- System & Information Integrity
- Program Management

CONFIDENTIAL

The California Cybersecurity Maturity Metrics (CCMM) developed by CDT OIS is a 0-4 scale that translates an entity's audit results into a numerical value. The target goal is to move the State to a CCMM score of 2 as a minimal baseline score. Although the CCMM includes a small portion of technical controls, most of it focuses on measuring the foundational elements of each entity's policy and compliance posture. The following chart breaks down each score range.

Implementation	4	The entity has achieved a greater degree of effectiveness in implementing its cyber security practices and procedures.
	3	The entity has implemented its cyber 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 cyber security program.
	1	The entity has developed the foundational elements of its cyber security program.
	0	The entity lacks the foundational elements required for a cyber security program.

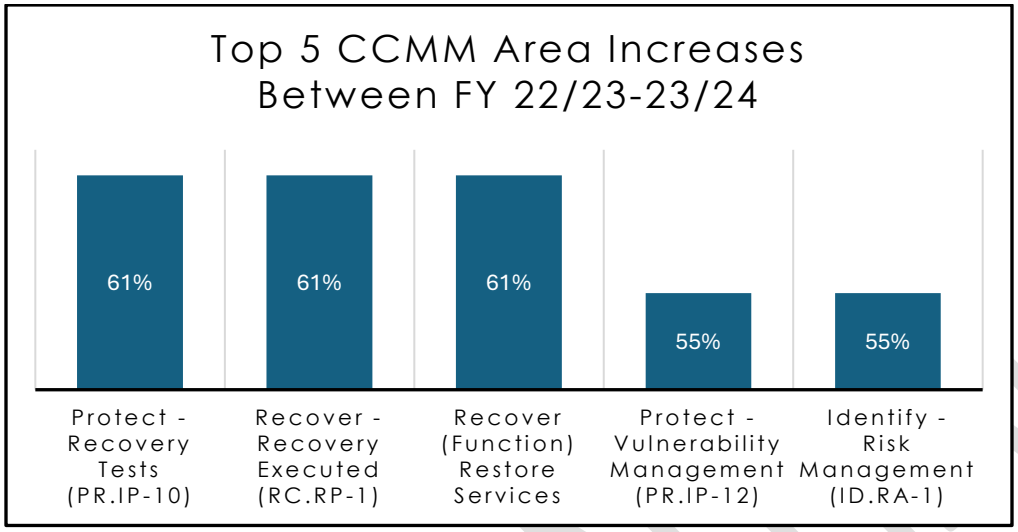
In FY 2022/23, the average score for state entities was 1.32, indicating that cybersecurity practices and procedures were implemented, but additional improvements were needed.



In FY 2023/24, the state's CCMM score improved by 0.52, resulting in an average score of 1.85. The increase demonstrates that entities effectively addressed the findings identified in audits and are strongly committed to improving overall cybersecurity posture.

CONFIDENTIAL

The areas that improved the most were response, recovery, vulnerability management, and risk management.



Despite increases across the state in vulnerability management and risk management, there are still significant opportunities for further improvement. Specifically, data protection and the distribution of cybersecurity policies remain areas of concern with lower score results.

The inadequate distribution of cybersecurity policies impedes the implementation of other policies throughout organizations. As an interim solution, CDT released several policy templates often identified as needing improvement by entities. By providing baseline templates and sample material, the cybersecurity community was able to save time and resources in developing their departmental policies.

Since the implementation of Cal-Secure, CDT increased its focus on sharing identified gaps with agencies through risk registers. This added visibility and empowered agencies to take a more active role in supporting the entities under their oversight. This policy is expected to play a key role in strengthening and improving the cybersecurity posture over time. These risk registers are currently in the form of static reports, but CDT is moving to an automated and dynamic reporting system to allow agencies access, as needed.

Lastly, CDT introduced a Virtual Chief Information Security Officer (vCISO) program to help aid and support statewide cybersecurity efforts. Specifically, the vCISO will support smaller entities requiring extra support to maintain statewide compliance and implement risk-mitigating cybersecurity controls. A vCISO provides the same strategic expertise as a traditional CISO but on a temporary basis. This program provides additional resources to smaller entities while exploring permanent solutions. To date, this program has closed more than 400 critical gaps in assisting entities in adopting and fully operationalizing Cal-Secure initiatives.

CONFIDENTIAL

Nationwide Cybersecurity Review

The Nationwide Cybersecurity Review (NCSR) is an annual, voluntary self-assessment for U.S. government agencies to evaluate cybersecurity practices. Developed by the Department of Homeland Security (DHS) and the Center for Internet Security (CIS), the NCSR assists state, local, tribal, and territorial entities in assessing cyber readiness by identifying strengths and gaps in their defenses.

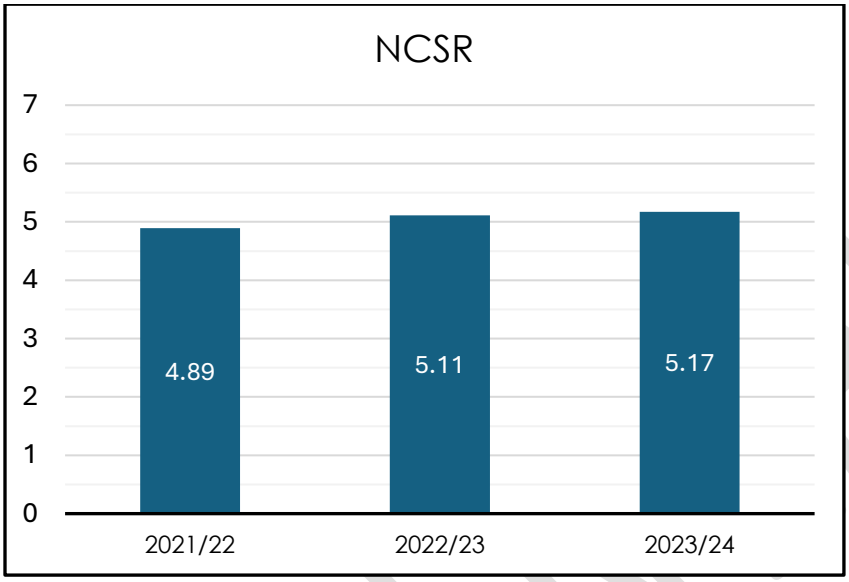
The questions in the NCSR survey serve as an important data point for measuring progress on the Cal-Secure roadmap. Approximately 50 percent of the 94 NCSR survey questions overlap with the 29 technical capabilities outlined in Cal-Secure. Specifically, 42 NCSR questions correspond to these capabilities. While NCSR encompasses broader topics beyond Cal-Secure's focus, this overlap makes NCSR scores valuable for tracking cybersecurity improvement and alignment with technical goals. A crosswalk between NCSR criteria and Cal-Secure technical capabilities can be found in Appendix B.

NCSR uses a seven-point maturity scale. The target is for Gov. Code Section 11546.1 entities to achieve a score above five.

Score	Maturity Level	Description
7	Optimized	Entity implements activities with documented policies, standards, & procedures, regularly testing & ensuring effectiveness.
6	Tested & Verified	Entity executes processes with formally documented policies, standards, & procedures, ensuring implementation is tested.
5	Implementation in Process	Entity has defined an activity or process within documented policies, standards, & procedures & is currently working to align this documentation with a formal security framework or methodology.
4	Partially Documented Procedures	Entity has established a formal policy & is in the process of developing documented standards & procedures to support it.
3	Documented Policy	Entity has an approved formal policy in place by management.
2	Informally Done	Activities & processes might be performed effectively, & suitable technologies might exist to achieve objectives; however, they remain undocumented & lack formal approval.
1	Not Performed	Activities, processes, & technologies are currently absent.

CONFIDENTIAL

Over the past three fiscal years, the average NCSR score across all state agencies and entities have gradually increased, reaching the target score of five. This indicates that many entities are in the implementation phase of their tools and technologies.



Overall, the California state agency NCSR results show strong performance in areas that correspond to the earlier priority 1 and 2 technical capabilities while also highlighting areas for improvement in the areas corresponding to priority 3, 4, and 5 capabilities.

CONFIDENTIAL

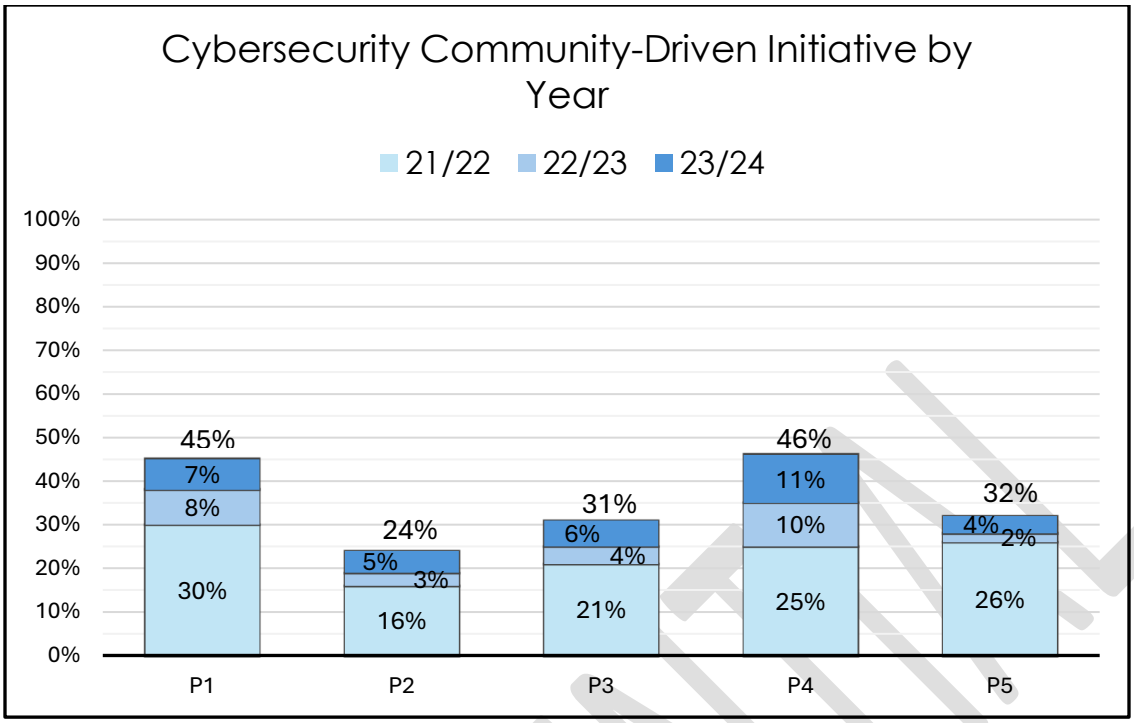
Cal-Secure Key Community-Driven Initiatives & Constraints

There are 15 Cal-Secure key initiatives. Although cybersecurity key initiatives are optional and community-driven, they are essential for fostering a stronger cybersecurity culture. These initiatives support technical capabilities by emphasizing the human element of cybersecurity, leading to more effective management and use of the tools required to implement the 29 technical controls.

Priority 1 FY 21/22	**Priority 2** FY 22/23	**Priority 3** FY 23/24	**Priority 4** FY 24/25	**Priority 5** FY 25/26
• Tailored Cybersecurity Workshops	• NICE Framework Alignment • Cybersecurity Career Toolkit • Cybersecurity Strategy Tools • Formalized Cybersecurity Governance • Multi-tiered Cybersecurity Governance Bodies	• Cybersecurity Development Programs • Cybersecurity Talent Pipelines • Modernized Cybersecurity Procurement • Defined Cybersecurity Technology Requirements	• Transformed Policies and Standards • Cybersecurity as a Service • SOC Services	• Unified Integrated Risk Management Platform • Secure IT Modernization

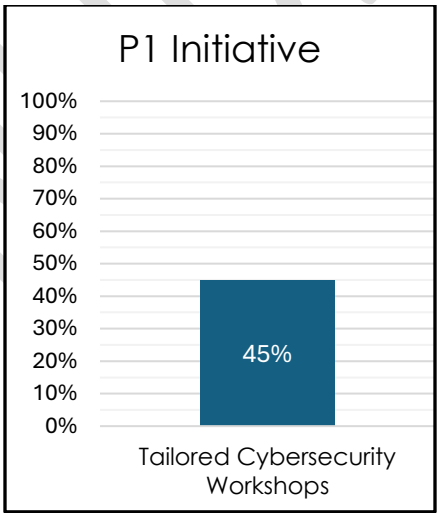
This chart shows the average progress of key initiatives implemented by all Gov. Code Section 11546.1 entities, highlighting advancements toward achieving the 15 initiatives per fiscal year. To make progress, agencies must get executive leadership support, plan, secure resources, and execute plans. This can include a combination of major programs and incremental improvements. The goal is to establish a foundational cybersecurity culture across the state.

CONFIDENTIAL



Key Initiative Priority 1 Progress

California state entities have implemented 45 percent of Priority 1 initiatives at the time of this report. CDT and Cal-CSIC provide two workshops per year to support entities as a stop-gap measure.



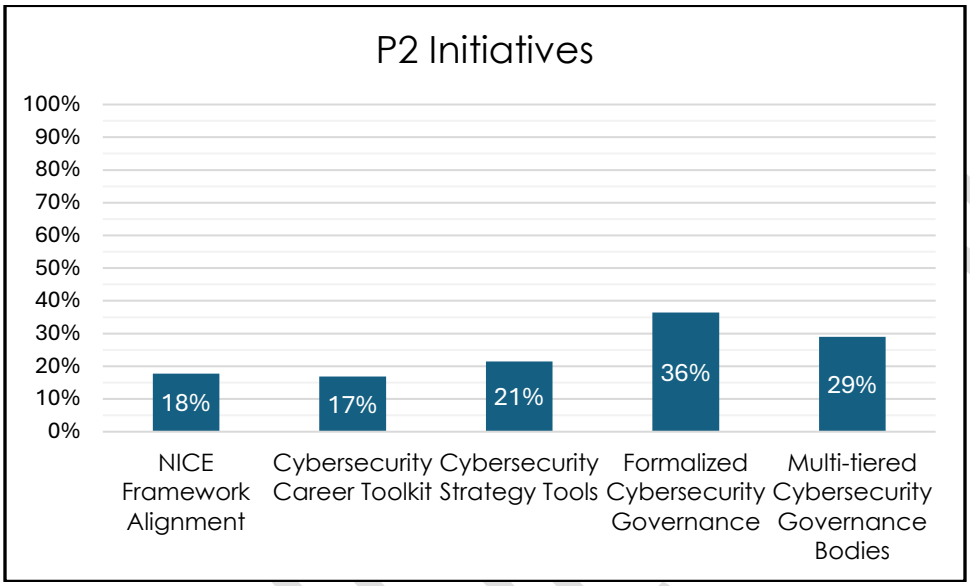
The biennial workshop series, Cyber Storm, simulates large-scale cyber-attacks on critical infrastructure and the government. These workshops focus on information sharing, coordination, and decision-making to improve cyber incident response capabilities. To augment tailored cybersecurity workshops such as Cyber Storm, the Cal-CSIC supports a cyber range. This controlled, interactive technological environment is an innovative cybersecurity tool where cybersecurity professionals of any skill level can learn and practice threat

CONFIDENTIAL

decision, as well as eradication techniques based on real-world scenarios. Currently, the Cal-CSIC's cyber range solution is provided by a top-tier cybersecurity vendor which includes monthly 3-day instructor-led workshops.

Key Initiative Priority 2 Progress

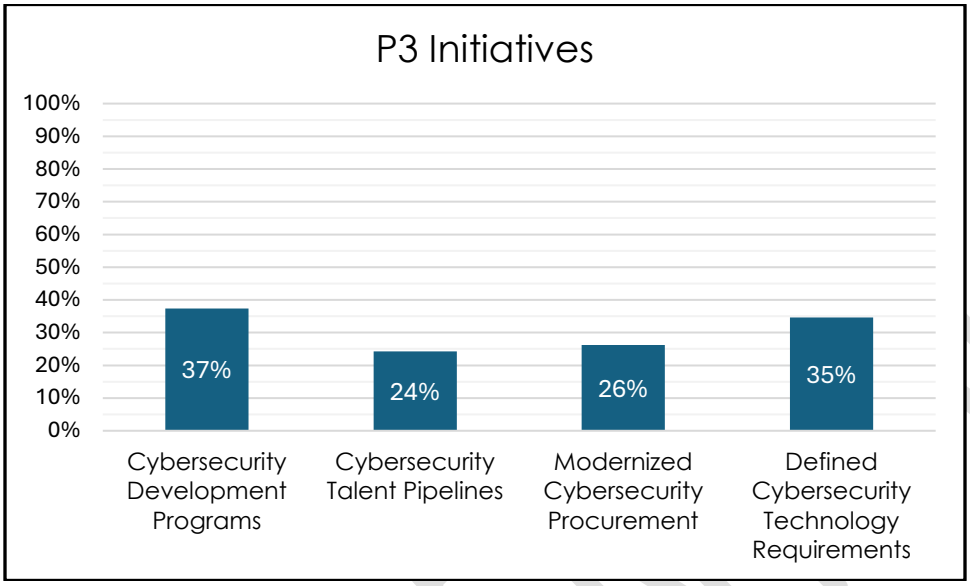
California state entities have implemented an average of 24 percent of Priority 2 initiatives at the time of this report.



As a culture-gap measure, CDT's Office of Professional Development works with state entity HR departments to disseminate guidance on cybersecurity workforce alignment with the National Initiative for Cybersecurity Education (NICE) framework. This guidance is meant to address cybersecurity knowledge, skills, and abilities within the state agency cybersecurity community. Additionally, CDT offers a Cyber Security Officer 101 and 102 Essentials courses that cover services and tools available to entities. Furthermore, CDT holds monthly Cyber Security Advisory Council meetings to improve cybersecurity collaboration across state agencies. These meetings include focused discussion on formalized cybersecurity governance and multi-tiered cybersecurity governance bodies.

Key Initiative Priority 3 Progress

California state agencies and entities have implemented an average of 31 percent of Priority 3 initiatives at the time of this report.

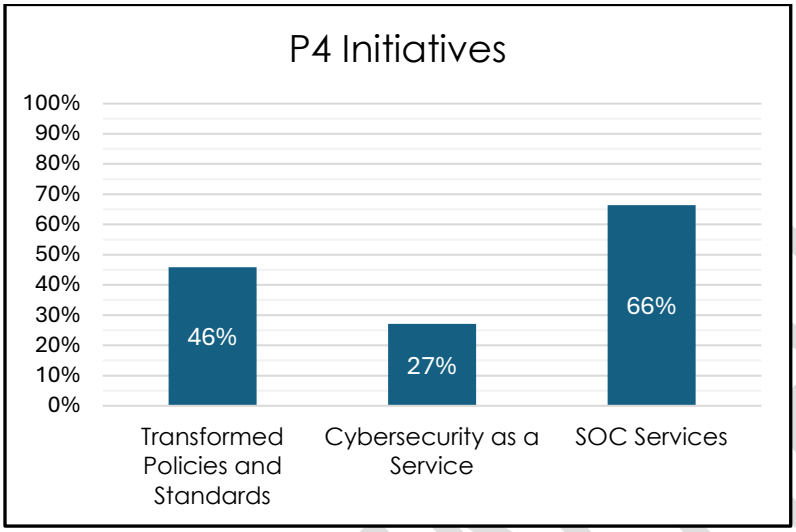


Cybersecurity is rapidly evolving, which requires constant updates to curriculum and increased awareness about the importance of cybersecurity at both individual and organizational levels. To bridge the gap, CDT and the Cal-CSIC participate in education summits to drive talent pipelines, work with procurement counterparts on implementing security requirements into contracts for procurement and collaborate on new policies and standards.

CONFIDENTIAL

Key Initiatives Priority 4 Progress

California state entities have implemented an average of 46 percent of Priority 4 initiatives by the end of the reporting period.

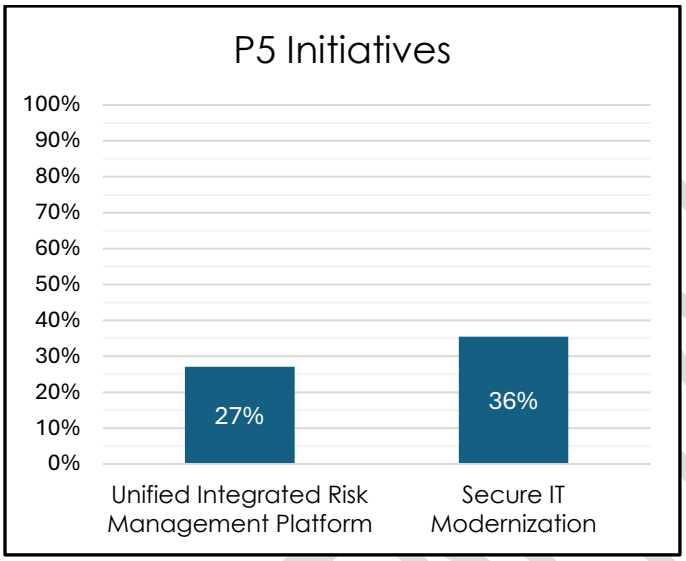


CDT offers Security Operations Center (SOC) services as a provisional fix and is working on putting out more policy templates and standards to provide a framework for entities to follow. SOC services include the setup and configuration of tools required for a Security Operations Center. A subset of those services includes SOC as a Service (SOCaaS), which focuses specifically on the ongoing operational monitoring of an entity's cybersecurity provided by the CDT SOC where an entity does not have its own SOC or full SOC capability yet.

CONFIDENTIAL

Key Initiatives Priority 5 Progress

California agencies and entities have implemented an average of 32 percent of Priority 5 initiatives by the end of the reporting period.

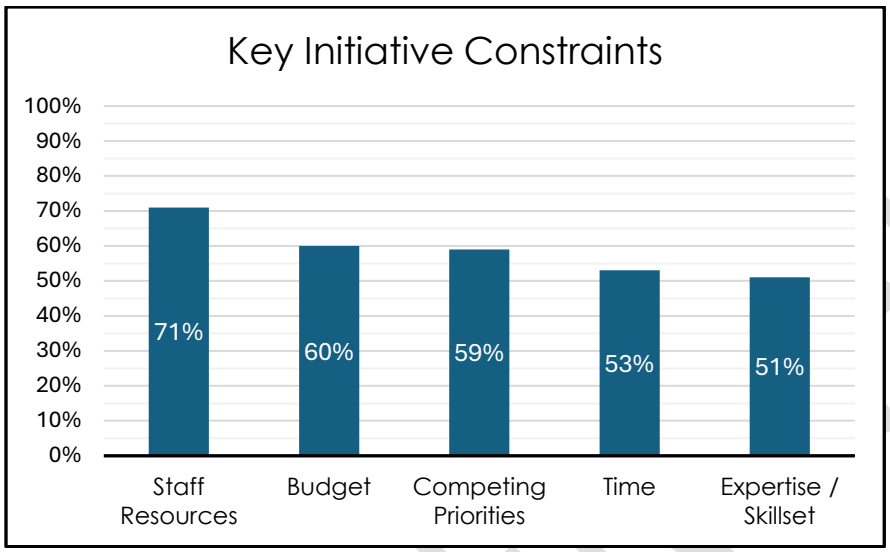


State entities are encouraged to implement a governance, risk, and compliance (GRC) platform or equivalent capability to further mature their information security program. This is in lieu of a statewide unified integrated risk management (UIRM) platform, which is not currently in place but may be in the future. For purposes of this evaluation and report, the number under UIRM represents implementation of GRC platforms or equivalent capability. As a collaborative effort, CDT works with state entities to provide guidance on requirements, standards, and best practices for GRC. This effort fosters seamless integration across agencies and the broader State of California, promoting consistent and baseline maturity for risk management and compliance practices.

CONFIDENTIAL

Key Initiatives Constraints

The chart below highlights the main constraints identified by state entities impacting community-driven initiatives. The categories are the same as those presented for technical capabilities, but the exact numbers (relative weights) are different.



Entities report that budgets and staff have been, and continue to be, significant barriers in achieving key initiatives. Competing priorities and time also hinder progress, reflecting a common theme of limited resources.

Overall, the data suggests that budget constraints and resource limitations are substantial challenges across both technical and initiative-focused capabilities, although slightly more so for technical capabilities.

CONFIDENTIAL

Funding & Positions

Assembly Bill 128 (Ting, Statutes of 2021, Budget Act of 2021) included a one-time, $11.3 million, and an ongoing $38.8 million to mature the state's overall security posture, improve statewide cybersecurity initiatives, analyze cyber threat intelligence, and mitigate potential threats. Through this funding, statewide cybersecurity programs were implemented by CDT such as the vCISO program and SOC as a Service (SOCaaS). As of FY 2023/24 approximately one-half of all state entities surveyed were using SOCaaS and this includes more than two thirds of agencies.

Funding statewide initiatives, which aim to close gaps and cyber deficiencies of the state, offer a greater return on investment in cybersecurity maturity than funding individual entities separately. As noted earlier, audits and assessments revealed that smaller departments often lack the resources and staff to effectively implement cybersecurity controls, leading to lower scores relative to medium and large entities. Statewide efforts help address these common challenges, delivering solutions that accelerate progress and benefit all entities simultaneously, rather than requiring each to develop capabilities in isolation. With the growing number of entities seeking assistance, CDT is carefully balancing demand with its available capacity to ensure effective service delivery. To continue meeting these needs, resource constraints will be addressed through state budget change proposal process.

The chart below shows the total security funding amount for FY2022/23 and FY 2023/24.

	2023-24			
	General Fund	Other Funds	Total	Pos
2022/23 Budget (Ongoing amount)	$ 57,741,000	$ 18,406,000	$ 76,147,000	157
2023/24 Budget (Year 1 and 2)	$ 56,634,000	$ 16,981,000	$ 73,615,000	111
			$ 149,762,000	268

The ongoing baseline funding from FY 2022/23 was $76.1 million for security efforts. In addition, the FY 2023/24 budget introduced new funding of $73.6 million bringing the total funding for security to $149.76 million across both fiscal years. The number of personnel also increased from 157 in FY 2022/23 to 268 in FY 2023/24 (increase of 111 positions).

Overall, FY 2023/24 reflects a notable increase in security funding, highlighting the state's ongoing commitment to enhance its security framework through the allocation of new resources in addition to the existing security funding baseline. However, in response to anticipated significant General Fund deficits, DOF issued Budget Letters 23-27 and 24-01, which implemented a temporary expenditure freeze in FY 2023/24. The 2024 Budget Act (Assembly Bill 107, Gabriel) included an unallocated reduction of 7.95 percent for operating expenses.

CONFIDENTIAL

To address budget constraints, CDT continues to collaborate with agencies to explore opportunities that can enhance security posture across multiple entities within each agency. This collaboration occurs on a quarterly basis led by OIS and covers a range of topics including ISAs, audits, TRPs, risk assessment and management, compliance, etc. These discussions aim to identify ways to allocate security funding more effectively in key focus areas, ensuring resources are used efficiently to strengthen overall security. The Cal-CSIC also regularly provides guidance to state agencies through incident response services or proactive recommendations and threat intelligence.

CONFIDENTIAL

Conclusion

Overall, California state entities have made significant progress on the implementation of Cal-Secure capabilities and initiatives. While much work remains, most state agencies are trending positively and substantially improving their cybersecurity posture. Cybersecurity is a rapidly evolving field, with known and unknown risks and emerging threats facing the state each day. The establishment of Cal-Secure has provided a solid foundation for state government to make meaningful improvements to secure the cyber landscape for the state. Additionally, the ongoing audits and assessments will allow the state to be nimble as it addresses new threats in the future. While it is hopeful that Cal-Secure be enough to keep pace with known risks and emerging threats facing the state in the cyber landscape, it will be difficult to determine exactly which resources and efficiencies could accelerate cybersecurity progress throughout the state.

As the cyber-threat landscape continue to evolve, the Cal-Secure roadmap maintains baseline efforts that will last, even as cybersecurity outpaces government capabilities. Continued implementation of all 29 technical capabilities, coupled with the 15 key initiatives, will be critical to California's cybersecurity posture and future. Moreover, the continued support of the state legislature remains critical as California continues to strengthen its cybersecurity efforts, through efforts such as the nation-leading Cal-CSIC. Yet, as this report details, there is still work to be done.

CONFIDENTIAL

Glossaries

Cal-Secure Roadmap Glossary

Anti-Malware Protection
The automated technical capability to detect and block malicious activity from trusted and untrusted applications and dynamically respond to security incidents and alerts.

Anti-Phishing Program
A collection of security controls, including technological capabilities to detect and prevent email-based phishing attacks, as well as the process of training employees to identify and deal with potential phishing email threats.

Application Development Security
Security as part of the software development lifecycle to ensure application confidentiality, integrity, and availability. It includes the people, processes, policies, and practices to build security into application development and is the responsibility of all stakeholders and project staff, not just the software developers.

Application Security
Application security incorporates specific security measures, policies, processes, and controls into all phases of the application lifecycle including design, development, testing, implementation, upgrade, and maintenance.

Application Whitelisting
The use of whitelists (a list of explicitly allowed applications) to control the applications permitted to execute on a host, thereby preventing the execution of malware, unlicensed software, and other unauthorized software.

Asset Management
The effective tracking and managing of IT assets for an entity's program and enterprise IT infrastructure and production systems, including the ability to identify and classify entity owned hardware and software, telecommunications, maintenance costs and expenditures, support requirements (e.g. state staff, vendor support), and the ongoing refresh activities necessary to maintain the entity's IT assets.

Cloud Security Monitoring
The continuous security monitoring of cloud infrastructure for potential security vulnerabilities and threats, as well as assuring optimal functioning of the cloud platform while minimizing security risks including costly data breaches.

CONFIDENTIAL

Continuous Patch Management
Systematic notification, identification, deployment, installation, and verification of operating system, firmware, and application software patches.

Continuous Vulnerability Management
Vulnerability Scanning is an inspection of potential points of exploit and weakness on a network or system including outdated software versions, missing patches or misconfigurations and flawed programming.

Cybersecurity as a Service
A model where cybersecurity services are provided on-demand by third-party vendors or service providers. This includes a variety of services, such as threat monitoring, incident response, vulnerability management, and more, delivered through the cloud or remote platforms. Organizations can leverage CaaS to enhance their cybersecurity capabilities without needing to build an internal security team.

Cybersecurity Career Toolkit
A set of resources, tools, and guidance designed to help individuals advance their careers in cybersecurity. This toolkit typically includes resume templates, certifications, skill development programs, job search strategies, interview preparation tips, and industry insights to support professionals in the cybersecurity field.

Cybersecurity Development Programs
Structured educational and training initiatives aimed at building or enhancing the cybersecurity skills of employees or aspiring cybersecurity professionals. These programs may include certifications, workshops, formal courses, and hands-on experiences to improve knowledge in areas such as threat detection, incident response, ethical hacking, and security management.

Cybersecurity Strategy Tools
A collection of methodologies, frameworks, and software tools designed to help organizations develop, implement, and monitor their cybersecurity strategy. These tools assist in risk assessment, policy development, threat analysis, and compliance management, enabling organizations to plan and execute effective cybersecurity initiatives.

Cybersecurity Talent Pipelines
The systematic process of attracting, developing, and retaining skilled cybersecurity professionals within an organization or industry. This involves partnerships with educational institutions, internships, mentorship programs, and professional development opportunities to ensure a steady flow of qualified candidates to fill cybersecurity roles.

CONFIDENTIAL

Data Loss Prevention
The ability to identify, monitor, and protect data in use (e.g. endpoint actions), data in motion (e.g. network actions), and data at rest (e.g. data storage) from unauthorized use and disclosure. DLP includes deep packet inspection and analyzing the contextual security of transactions.

Defined Cybersecurity Technology Requirements
A formal set of specifications and guidelines that outline the technical standards, tools, and security controls that an organization must implement to protect its digital infrastructure from cyber threats. These requirements help ensure consistency and alignment with cybersecurity goals.

Disaster Recovery
The ability of an organization to respond to a disaster or an interruption in services by implementing a disaster recovery plan to stabilize and restore the organization's critical functions.

Enterprise Encryption
Enterprise encryption applies security and access controls directly to structured and unstructured data wherever it exists in the enterprise including on premises, virtual, in the cloud or in a hybrid environment, and at rest, in transit and in motion.

Enterprise Sign-On
Enterprise sign-on eliminates the need to separately authenticate and sign-on to individual applications and systems. It allows the user to authenticate once and then be subsequently and automatically authenticated when accessing other specified systems.

Formalized Cybersecurity Governance
The establishment of structured, well-documented processes, policies, and roles to manage and oversee cybersecurity efforts across an organization. This typically involves creating frameworks for decision-making, accountability, and monitoring compliance with security policies.

Identity Lifecycle Management
The collection of technologies and practices that provisions and deprovisions users to appropriate levels of access to organizational resources.

Incident Response
An action plan for dealing with intrusions, cyber-theft, denial of service, fire, floods, and other security-related events. It is a six-step process: 1) preparation, 2) identification, 3) containment, 4) eradication, 5) recovery, and 6) lessons learned.

CONFIDENTIAL

Insider Threat Detection
A coordinated collection of security capabilities designed to detect the unauthorized disclosure of sensitive information by an entity with authorized access.

Log Management
The process for generating, transmitting, storing, analyzing, and disposing of log data. Log management is essential to ensure computer security records are stored in sufficient detail for an appropriate duration. Sources of log entries include network devices, authentication servers, operating systems, applications, etc.

Mobile Device Management
The fundamental visibility and security controls needed to secure, manage, and monitor any entity or employee-owned mobile device, such as smartphones or tablets that access an organization's sensitive or confidential information.

Mobile Threat Defense
Threat detection and protection technologies designed for the requirements and vulnerabilities of mobile platforms, such as smart phones and tablets.

Modernized Cybersecurity Procurement
The process of updating and optimizing how an organization acquires cybersecurity tools, services, and technologies. This can involve streamlining vendor selection, integrating new technologies, and ensuring that procurement processes keep pace with emerging cybersecurity threats.

Multi-Factor Authentication
Authentication based on two or more of the following: something you know (i.e. password), something you have (i.e. token or smartcard), or something you are (i.e. a biometric).

Multi-Tiered Cybersecurity Governance Bodies
A structured hierarchy of committees or groups responsible for overseeing various aspects of cybersecurity within an organization. This can include different governance levels (e.g., executive, operational, technical) that work together to ensure that cybersecurity strategies are properly implemented and aligned with organizational goals.

Network Access Control
Examining incoming connections to an organization's network from remote users and allow or disallow access based on those checks.

CONFIDENTIAL

Network Threat Detection
Effective monitoring and analyzing of network or system events to find, and provide real-time or near real-time warning of, attempts to access-system resources in an unauthorized manner.

Network Threat Protection
Effective protection against network security threats attempting to harm organizational assets and thwarting attempts to proliferate on an organization's network.

NICE - National Initiative for Cybersecurity Education
The NICE framework describes cybersecurity work, and the knowledge, skills, and abilities (KSAs) needed to complete tasks that can strengthen the cybersecurity posture of an organization and improve communication about how to identify, recruit, develop, and retain cybersecurity talent.

Operational Technology Security
Operational Technology is hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes, and events in the enterprise. OT is common critical infrastructure in Industrial Control Systems (ICS) such as a SCADA System.

Privileged Access Management
Secure provisioning of privileged access to critical assets, and effective monitoring and maintenance of privileged accounts and access. Privileged access spans a wide range of systems and infrastructure components, such as operating systems, databases, middleware, applications, and network devices.

Secure IT Modernization
The process of upgrading and enhancing an organization's IT systems and infrastructure in a way that prioritizes security. This includes integrating new technologies, replacing outdated systems, and ensuring that modernization efforts adhere to cybersecurity best practices.

Security and Privacy Awareness Training
Educational programs designed to increase employees' and stakeholders' knowledge about cybersecurity threats, best practices for protecting data, and compliance with privacy regulations. The goal is to create a culture of security awareness and help individuals recognize and respond to potential security incidents.

Security Continuous Monitoring
Cyber Security Continuous Monitoring is the ongoing monitoring sufficient to ensure and assure effectiveness of security controls related to systems and networks by assessing security control implementation and organizational security status in accordance with organizational risk tolerance and within a

CONFIDENTIAL

reporting structure designed to make real-time, data-driven risk management decisions.

SOC Services (Security Operations Center Services)
A set of services provided by a dedicated team or an external provider responsible for continuously monitoring, detecting, and responding to security threats and incidents within an organization. The SOC ensures real-time cybersecurity vigilance through threat intelligence, incident response, and security event monitoring.

Software Supply Chain Management
The process of overseeing and securing the sourcing, development, and delivery of software throughout its lifecycle. This includes ensuring that third-party components, open-source code, and software updates are secure and free of vulnerabilities that could expose an organization to cyber risks.

Tailored Cybersecurity Workshops
Customized training sessions or interactive events that are designed to address the specific cybersecurity needs and challenges of an organization or group. These workshops are typically aimed at educating teams on particular security issues or improving their ability to manage security risks.

Threat Intelligence Platform
Automated mechanism to aggregate, transform, analyze, interpret, or enrich threat information to provide the necessary context for decision-making processes.

Transformed Policies and Standards
The process of reviewing, updating, and overhauling an organization's cybersecurity policies and standards to align with current threats, regulatory requirements, and industry best practices. This transformation ensures that security protocols are effective, up-to-date, and relevant to the organization's needs.

Unified Integrated Risk Management Platform
A platform to simplify, automate, and integrate enterprise, operational, and IT risk management processes and data to make better-informed risk-based decisions.

CONFIDENTIAL

Independent Security Assessment Glossary

10.1 – Account Naming Standards for Role-based Separation
This task specifically checks for a process or indication that allows for the unique identification of privilege role accounts when viewing standard user accounts. The entity must demonstrate it identifies unique naming conventions across the various account types – privileged accounts, service accounts, and standard user accounts.

10.2 – Least Privilege Assessment of Key Roles
This task reviews the entity's enterprise to determine if standard user accounts have privileged roles membership. The entity is assessed to validate that it demonstrates the practice of separate account provisioning for privileged roles as part of its Principle of Least Privilege management.

10.3 – Least Privilege Assessment of Key Hosts
This task evaluates a random subset of hosts within the entity's enterprise to assess the presence of any standard user accounts within the contained privileged roles on the target host. The entity is assessed to validate the implementation of the Principle of Least Privilege which requires the separation of provisioned standard user and privileged account access rights between two or more distinct accounts, as applicable.

10.4 – FIPS Compliant Remote Access Solution Validation
This task validates that network-level connections from external networks (e.g., VPN, VDI, etc.) require a FIPS 140-2 approved encryption implementation configuration and certification. The entity's deployed remote access solution must be FIPS compliant and operating in FIPS mode as part of the measured standard.

10.5 – Account Testing of Applied Controls for Privileged User Access
Password-based authentication is a type of authenticator that can support authenticator management. This task validates the enforcement of password settings and restrictions for privileged accounts by the application of strong characteristics for privileged account types – interactive and non-interactive logon. When privileged users are assigned rights used to perform system administration, configuration, or privilege escalation, their credentials are typically utilized as interactive logons. When privileged access is assigned to role-based functions such as service accounts, users are not expected to utilize the account as part of their routine duties; therefore, these accounts are classified as non-interactive logons.

10.6 – Account Testing of Applied Controls for Standard User Access
Password-based authentication is a type of authenticator that can support authenticator management. This task validates the enforcement of password

CONFIDENTIAL

settings and restrictions for non-privileged accounts by the application of strong password characteristics via implementation of fine-grained password policies.

10.7 – Remote Access Solutions Protected by Multi-Factor Authentication (MFA)
Remote access is defined as the presentation of non-public logical access from locations external to entity security control. This task validates that the entity enforces NIST 800-63-2 compliant Multi-factor Authentication (MFA or 2FA). The entity must meet the following conditions for all remote access solutions.

10.8 – Risk Analysis Team Conducted User Phishing Practical Exercise
This task tests user participation in an unannounced simulated phishing exercise. The entity must provide required user information in accordance with assessment standards and configuration requirements.

11.1 – Cloud Security Configuration Management
This task validates that the entity applies automated cloud cybersecurity assessment measurements to each 3rd party cloud-operated environment. Using score results, the entity must perform continuous monitoring of compliance, applying security recommendations to reduce risk exposures while maintaining business process operability, achieving a baseline secure configuration score.

11.2 – Baseline Image Security Configuration and Analysis
This task measures the application of system hardening controls/settings of entity on-premises and cloud-based systems. System hardening is assessed via the percentage of compliance against the NIST Moderate standard (as applicable based on available host template) for the hosts listed below. Provided hosts must include a representative subset of operating systems, as available.

11.3 – Continuous Surveillance for At-Risk Service Exposure
Routine evaluation of the entity host/service exposures should be a part of the entity's continuous risk assessment and evaluation process. This task validates that the entity conducts monthly scans (at a minimum) of all hosts/devices to determine their service exposures.

12.1 – Boundary Protection Solutions Prohibit Insecure Management Protocols
This task validates that the entity perimeter firewall (entity or hosting activity as applicable) restricts insecure protocol usage on the management interface to prevent unauthorized access and information leaks.

12.2 – Endpoint Security Deployment and Monitoring
The entity deploys endpoint protection on all entity managed hosts within its control (on-premises, 3rd party hosted, and cloud). For entities utilizing endpoint protection solutions managed via Active Directory (AD) membership, a separate enterprise management console must be provided for non-domain

CONFIDENTIAL

joined/stand-alone assets if they cannot be managed within a single enterprise solution.

12.3 – Detection and Mitigation of Network Rogue Devices
This task measures the ability of the entity to detect and mitigate unauthorized (rogue) device connections within the enterprise. The entity must deploy controls and monitor network for signs of network connected rogue devices, must confirm rogue device presence, and takes steps to disable network access and remove from network.

12.4 – Host Scans for Continuous Monitoring and Vulnerability Management
The entity must provide proof of recurring, privileged access authenticated vulnerability scans. Scans must be sufficient to validate the status of system and installed application security patch states (including 3rd party security patching) on all systems under entity control (physical, virtual, cloud-hosted) as part of the entity continuous vulnerability monitoring program.

12.5 – Secure DNS Communication through CDT Managed Infrastructure
This task measures how entity DNS internal requests are routed. Entities should ensure requests and responses are logged by entity perimeter security devices prior to being forwarded to CDT managed DNS resolvers. A Deny All, Permit by Exception (DAPE) DNS isolation policy must be in place to prohibit internal DNS queries from direct DNS root server query. This logical control enforces entity's DNS queries are routed and inspected by the CDT SOC. Any direct routing or CDT secure DNS bypass fails this task standard.

13.1 – Boundary Protection Ingress/Egress Monitoring
The entity must conduct network monitoring using firewalls and intrusion detection/prevention systems of all ingress/egress points to the network. This task requires entities to demonstrate intrusion monitoring through device console access (3rd party/CDT managed devices require SLA/Statement of Boundary Protection).

13.2 – Boundary Protection Device Deployed in a Best Practice Configuration
This task will perform an analysis of the primary boundary protection firewall rules.

- Rules are implemented using a Deny All, Allow by Exception (DAPE) configuration.
- Exceptions are specific to the minimum IPs and ports/protocols/applications required by role/host function.
- The absence of unnecessary services allowed between externally accessible segments and their hosts (e.g., "any" rules between external or DMZ segments).
- Firewall conformed to the manufacture security best business practices.

CONFIDENTIAL

- Score overall firewall security rating is inclusive of at-risk rules, excessive ports/protocols, and best practices; security rating results are scaled from 1-100 percent.

13.3 – IDS/IPS Event Monitoring, Review and Clearance/Escalation Procedures
Intrusion detection/prevention controls should be in place for entity/3rd party provider to monitor, review, and conduct clearance/escalation of anomalous network events. The entity (or 3rd party management) must conduct routine reviews of all on-premises and cloud security appliances.

13.4 – IDS/IPS Signature & Firmware Update
This task validates that the entity ensures the protection of hosts via maintenance of network IDS/IPS.

13.5 – SSL/SSH Traffic Inspection and Analysis
This task validates that the entity enforces all SSL/SSH traffic entering or exiting the network through a break and inspect proxy.

13.6 – Reoccurring Primary External Website Analysis
This task assesses the entity's analysis of its primary public external web site/application no less than quarterly. Assessment detects at-risk configurations, end-of-life applications, information leaks, and other security risks related to the provisioning of the content and data rendered. Scans must cover the assessment of common web application vulnerabilities.

14.1 – Entity Log Generation and Retention (6mo+)
This task validates that the entity generates and retains the required minimum key audit logs identified for a period of 6 months or longer.

15.1 – Distribution of Cybersecurity Alerts, Messages, and Warnings
This task determines whether the entity documents subscription to CDT (e.g., Cal-CSIRS notifications), Cal-CSIC (Intelligence Bulletins), Government notification list servers, and industry cybersecurity notifications to stay updated on current threat tactics. The entity must provide timely distribution of relevant received alerts/notifications to appropriate (cleared) internal communities of interest.

16.1 – Penetration Test External Open-Source Metadata Identity Collection
This task identifies the entity's risk exposure to publicly available identity-based metadata pertaining to its users past and present. This information provides attackers insight into valid usernames, valid email addresses and format, applications in use, and associated users with business function. Using these collected data points, the attacker can more effectively form password spraying and spear phishing attacks against the target entity. The Pen Test team

CONFIDENTIAL

will use active and passive reconnaissance techniques to acquire relevant and actionable information where possible.

16.2 – Penetration Test External Spear Phishing Attempt
This task assesses the entity's ability to react to a simulated threat actor directed spear phishing campaign derived from data collected via public/open sources only. This campaign must attempt to acquire credentials and may include a malicious code execution component. All campaigns by CND are initiated during the entity's normal business hours.

16.3 – Penetration Test External Password Guessing Activities
This task simulates a threat actor's ability to derive logon credentials while external to the entity network using brute force techniques including password spraying and password guessing. This process can include informed guessing via resources such as vendor documentation, key phrases on public websites, common passwords, and password dumps from public sources.

16.4 – Penetration Test External Credential Hash Capture and Cracking Operations
This task will assess the entity's risk exposure to Man-in-the-Middle authenticator hash capture, hash harvesting from exploited hosts, and extraction of authenticator hashes from network directory services. Captured hashes will be subjected to offline cracking attempts using dictionary and brute force attack methods for a period not to exceed the assessment period to assess cracking resistance.

16.5 – Penetration Test External Undeclared Hosts/Networks
This task simulates a threat actor's attempt to gather information about the victim's networks as part of their pre-attack, targeting phase. To validate the entity's knowledge and documentation of allocation assets/networks, a comparison of network exposures in the pre-attack phase is compared to the entity Data Call provided prior to assessment start date.

16.6 – Penetration Test External High-Risk Service Exposure Detection
This task assesses the entity's exposure of High-risk services to the internet. Using results from various service analysis techniques of in-scope and undeclared assets, the CND will identify any detected instances of services.

16.7 – Penetration Test External Host Management Service Detection
This task identifies poorly secured host management services and web application administrative interfaces exposed to the internet. This entity external network must be absent of any instance of externally exposed services.

16.8 – Penetration Test External Web Application Misconfigurations and Exposures

CONFIDENTIAL

This task identifies and probes selected in-scope and undeclared external websites and web applications to determine potential attack opportunities. Research and analysis are conducted to identify exploits and misconfigurations, achieve unauthorized access, detect non-public data exposure, and/or obtain unauthorized remote host access.

16.9 – Penetration Test External Execution of Malicious Code on Controlled Host
The successful exploitation of hosts or services operated, controlled, or provided via 3rd party to the entity. Exploitation of hosts must occur via the introduction of malicious code execution or host misconfiguration.

17.1 – Penetration Test Internal Password Guessing, Spraying, and Default Credential Detection
This task addresses two unique methods of obtaining passwords – password guessing and password spraying. Password spraying is the process of using informed knowledge such as acquired usernames in combination with common password dictionaries or common entity terminology to guess a username/password combination using brute force techniques. Default credential testing, when password guessing, utilizes well-known, often public information from application/hardware manufactures installation manuals to inform password guessing attempts on the targeted application/host.

17.2 – Penetration Test Internal Credential Hash Capture and Cracking
This task will assess the entity's risk exposure to Man-in-the-Middle authenticator hash capture, hash harvesting from exploited hosts, and extraction of authenticator hashes from network directory services. Captured hashes will be subjected to offline cracking attempts using dictionary and brute force attack methods for a period not to exceed the assessment period to assess cracking resistance.

17.3 – Penetration Test Internal Use of Insecure Host Management Services
This task attempts to identify any management service/interface that allows unencrypted access, weak encryption services, utilizes well-known community strings, or can be exploited using remote code execution methods places the entity at enhanced risk.

17.4 – Penetration Test Internal Web Site/Application Risks
This task identifies and probes selected in-scope and undeclared, internal websites and web applications to determine potential attack opportunities. Research of web risks and analysis are conducted to identify exploits and misconfigurations, achieve unauthorized access, detect non-public data exposure, or obtain unauthorized remote host access.

17.5 – Penetration Test Internal Wireless Network Breach Resistance
This task assesses the entity's protection of their wireless access at the network perimeter. The successful breach of a wireless network requires the capture of

CONFIDENTIAL

the 4-way handshake between any client and access point. This data provides a hash value of the credentials required for authentication. Once captured, a series of dictionary and brute force attacks on the hash can be performed to attempt to crack the password.

17.6 – Penetration Test Internal Execution of Code on Controlled Host

This task attempts the successful exploitation of entity hosts or services. Entity hosts or services are defined as entity controlled, operated, or hosts/services provided via 3rd party. Exploitation of hosts must occur via the introduction of code execution or host misconfiguration.

CONFIDENTIAL

California Cybersecurity Maturity Metric Glossary

Access Control (AC)
Controls in this family focus on limiting information system access and ensuring authorized use, and they require policies and procedures for managing access.
Awareness and Training (AT) This family involves training personnel on security awareness and best practices. Policies and procedures are needed to guide the training program.

Audit and Accountability (AU)
This family covers auditing and monitoring activities. Organizations must establish policies for auditing and accountability mechanisms.

Security Assessment and Authorization (CA)
The CA family involves policies and procedures for the ongoing assessment and authorization of systems, ensuring they meet security requirements.

Configuration Management (CM)
Configuration management policies guide the secure configuration of systems. Procedures ensure changes are tracked and approved.

Contingency Planning (CP)
Contingency planning controls require policies and procedures for disaster recovery and continuity of operations in case of system disruption.

Identification and Authentication (IA)
The IA family requires procedures for establishing and managing identities and authenticating users before granting access to systems.

Incident Response (IR)
Incident response policies and procedures dictate how to handle cybersecurity incidents, ensuring a planned and coordinated response.

Maintenance (MA)
This family addresses policies related to the maintenance of systems and procedures for controlling and managing maintenance activities.

Media Protection (MP)
Media protection policies and procedures ensure that data is properly stored, handled, and disposed of securely.

Physical and Environmental Protection (PE)
This family includes policies for controlling physical access to systems and procedures to secure the environmental conditions surrounding them.

CONFIDENTIAL

Planning (PL)
The Planning family involves high-level security and system planning policies. It ensures that security policies align with the organization's overall strategy.

Personnel Security (PS)
This family requires policies for managing personnel security and procedures for hiring, training, and managing employees to prevent insider threats.

Risk Assessment (RA)
Risk management policies help guide how an organization assesses and mitigates risk.

System and Services Acquisition (SA)
Acquisition policies govern the procurement of IT systems and services, ensuring security is considered during acquisition.

System and Communications Protection (SC)
This family includes procedures for securing information in transit and storage, requiring related policies.

System and Information Integrity (SI)
Policies for ensuring the integrity of systems and information are central in this family, with procedures to manage vulnerabilities and security issues.

Program Management (PM)
This control family includes policies and procedures to manage the overall security program at the organizational level.

CONFIDENTIAL

Appendix A: ISA Criteria & Cal-Secure Roadmap Mappings

#	ISA Criteria	Cal-Secure Technical Controls
1	10.1 – Account Naming Standards for Role-based Separation	Priority 2 - Privileged Access Management
2	10.2 – Least Privilege Assessment of Key Roles	Priority 2 - Privileged Access Management
3	10.3 – Least Privilege Assessment of Key Hosts	Priority 2 - Privileged Access Management
4	10.4 – FIPS Compliant Remote Access Solution Validation	Priority 4 - Enterprise Sign-on
5	10.5 – Account Testing of Applied Controls for Privileged User Access	Priority 2 - Privileged Access Management
6	10.6 – Account Testing of Applied Controls for Standard User Access	Priority 2 - Privileged Access Management
7	10.7 – Remote Access Solutions Protected by Multi-Factor Authentication (MFA)	Priority 1, Priority 4 - Multi-Factor Authentication, Mobile Device Management
8	10.8 – Risk Analysis Team Conducted User Phishing Practical Exercise	Priority 1, Priority 2 - Anti-Phishing Program, Security & Privacy Awareness Training
9	11.1 – Cloud Security Configuration Management	Priority 2, Priority 4 - Cloud Security Monitoring, Software Supply Chain Management
10	11.2 – Baseline Image Security Configuration and Analysis	Priority 4 - Application Development Security
11	11.3 – Continuous Surveillance for At-Risk Service Exposure	Priority 2 - Security Continuous Monitoring
12	12.1 – Boundary Protection Solutions Prohibit Insecure Management Protocols	Priority 3 - Operational Technology Security
13	12.2 – Endpoint Security Deployment and Monitoring	Priority 5, Priority 4 - Insider Threat Detection, Mobile Device Management
14	12.3 – Detection and Mitigation of Network Rogue Devices	Priority 3, Priority 5 - Network Threat Detection, Mobile Threat Defense
15	12.4 – Host Scans for Continuous Monitoring and Vulnerability Management	Priority 1, Priority 4 - Continuous Vulnerability Management, Application Whitelisting
16	12.5 – Secure DNS Communication through CDT Managed Infrastructure	Priority 5 - Network Access Control
17	13.1 – Boundary Protection Ingress/Egress Monitoring	Priority 3 - Data Loss Protection, Disaster Recovery
18	13.2 – Boundary Protection Device Deployed in an Industry Best Practice Configuration	Priority 3 - Network Threat Protection
19	13.3 – IDS/IPS Event Monitoring, Review and Clearance/Escalation Procedures	Priority 2 - Incident Response
20	13.4 – IDS/IPS Signature & Firmware Update	Priority 2 - Continuous Patch Management
21	13.5 – SSL/SSH Traffic Inspection and Analysis	Priority 5 - Enterprise Encryption
22	13.6 – Reoccurring Primary External Website Analysis	Priority 3 - Application Security
23	14.1 – Entity Log Generation and Retention (6mo+)	Priority 3, Priority 4 - Log Management, Disaster Recovery
24	15.1 – Distribution of Cybersecurity Alerts, Messages, and Warnings	Priority 3 - Threat Intelligence Platform

CONFIDENTIAL

25	16.1 – Penetration Test External Open-Source Metadata Identity Collection	Priority 3 - Threat Intelligence Platform
26	16.2 – Penetration Test External Spear Phishing Attempt	Priority 1, Priority 2 - Anti-Phishing Program, Security & Privacy Awareness Training
27	16.3 – Penetration Test External Password Guessing Activities	Priority 2 - Privileged Access Management
28	16.4 – Penetration Test External Credential Hash Capture and Cracking Operations	Priority 5 - Identity Lifecycle Management
29	16.5 – Penetration Test External Undeclared Hosts/Networks	Priority 2 - Asset Management
30	16.6 – Penetration Test External High-Risk Service Exposure Detection	Priority 1 - Continuous Vulnerability Management
31	16.7 – Penetration Test External Host Management Service Detection	Priority 2 - Privileged Access Management
32	16.8 – Penetration Test External Web Application Misconfigurations and Exposures	Priority 3 - Application Security
33	16.9 – Penetration Test External Execution of Malicious Code on Controlled Host	Priority 1 - Anti-Malware Protection
34	17.1 – Penetration Test Internal Password Guessing, Spraying, and Default Credential Detection	Priority 5 - Identity Lifecycle Management
35	17.2 – Penetration Test Internal Credential Hash Capture and Cracking	Priority 5 - Identity Lifecycle Management
36	17.3 – Penetration Test Internal Use of Insecure Host Management Services	Priority 2 - Privileged Access Management
37	17.4 – Penetration Test Internal Web Site/Application Risks	Priority 3, Priority 4 - Application Security, Disaster Recovery
38	17.5 – Penetration Test Internal Wireless Network Breach Resistance	Priority 3 - Network Threat Detection
39	17.6 – Penetration Test Internal Execution of Code on Controlled Host	Priority 1 - Anti-Malware Protection

CONFIDENTIAL

Appendix B: NCSR Criteria & Cal-Secure Roadmap Mapping

	Cal-Secure Roadmap	NCSR Survey Question Areas
1	Priority 1 - Anti-Malware Protection	PR-DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.
2	Priority 1 - Anti-Phishing Program	PR-AT-1: All users are informed and trained; PR-AT-2: Privileged users understand roles and responsibilities (training on phishing awareness).
3	Priority 1 - Multi-Factor Authentication	PR-AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.
4	Priority 1 - Continuous Vulnerability Management	PR-IP-12: A vulnerability management plan is developed and implemented.
5	Priority 2 - Asset Management	ID-AM-1: Physical devices and systems within the organization are inventoried; ID-AM-2: Software platforms and applications are inventoried.
6	Priority 2 - Incident Response	RS-RP-1: Response plan is executed during or after an event; RS-AN-1: Notifications from detection systems are investigated.
7	Priority 2 - Continuous Patch Management	PR-IP-3: Configuration change control processes are in place.
8	Priority 2 - Privileged Access Management (PAM)	PR-AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.
9	Priority 2 - Security and Privacy Awareness Training	PR-AT-1: All users are informed and trained; PR-AT-3: Third-party stakeholders understand roles and responsibilities.
10	Priority 2 - Security Continuous Monitoring	DE-CM-1: The network is monitored to detect potential cybersecurity events; DE-CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.
11	Priority 2 - Cloud Security Monitoring	PR-DS-7: The development and testing environment(s) are separate from the production environment.
12	Priority 3 - Data Loss Prevention	PR-DS-5: Protections against data leaks are implemented; PR-DS-1: Data-at-rest is protected.
13	Priority 3 - Log Management	PR-PT-1: Audit-log records are determined, documented, implemented, and reviewed in accordance with policy.
14	Priority 3 - Network Threat Detection	DE-AE-2: Detected events are analyzed to understand attack targets and methods; DE-CM-1: The network is monitored to detect potential cybersecurity events.
15	Priority 3 - Network Threat Protection	PR-AC-5: Network integrity is protected (e.g., network segregation, network segmentation).
16	Priority 3 - Threat Intelligence Platform	ID-RA-2: Cyber threat and vulnerability information is received from information-sharing forums and sources.
17	Priority 3 - Application Security	PR-IP-1: A baseline configuration of information technology systems is created and maintained; PR-IP-2: A System Development Life Cycle to manage systems is implemented.
18	Priority 3 - Operational Technology Security	PR-IP-7: Protection processes are improved; PR-AC-1: Identities and credentials are issued, managed, verified, revoked, and audited.

CONFIDENTIAL

	Cal-Secure Roadmap	NCSR Survey Question Areas
19	Priority 4 - Disaster Recovery	PR-IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place.
20	Priority 4 - Enterprise Sign-On	PR-AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.
21	Priority 4 - Mobile Device Management (MDM)	PR-AC-3: Remote access is managed; PR-DS-3: Assets are formally managed throughout removal, transfers, and disposition.
22	Priority 4 - Application Development Security	PR-IP-2: A System Development Life Cycle to manage systems is implemented.
23	Priority 4 - Application Whitelisting	PR-AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.
24	Priority 4 - Software Supply Chain Management	ID-BE-1: The organization's role in the supply chain is identified and communicated; ID-BE-3: Priorities for organizational mission, objectives, and activities are established and communicated.
25	Priority 5 - Identity Lifecycle Management	PR-AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.
26	Priority 5 - Insider Threat Detection	DE-CM-3: Personnel activity is monitored to detect potential cybersecurity events; RS-CO-1: Personnel know their roles and order of operations when a response is needed.
27	Priority 5 - Network Access Control (NAC)	PR-AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.
28	Priority 5 - Enterprise Encryption	PR-DS-1: Data-at-rest is protected; PR-DS-2: Data-in-transit is protected.
29	Priority 5 - Mobile Threat Defense	PR-AC-3: Remote access is managed.

CONFIDENTIAL

Appendix C: Cal-Secure Technical Capability Completion Score Definitions

These ranges for completion of Cal-Secure technical capabilities could be viewed as maturity levels, comparable to ISA and NCSR criteria and CSF Tiers.

Score	Description
0 - 49%	Entities scoring in this range have significant deficiencies in their cybersecurity measures. This may indicate minimal implementation of security controls, leaving the organization highly vulnerable to cyber threats. They are likely not compliant with basic standards, and their overall security posture is weak, with a high risk of breaches or incidents.
50 - 59%	Entities scoring in this range have started to implement basic cybersecurity measures, but these are insufficient to provide adequate protection. While some security controls may be in place, there are significant gaps in coverage, leaving the organization exposed to substantial risks. These gaps could be in areas like access control, encryption, or monitoring, requiring immediate attention.
60 - 69%	This range reflects entities that meet the minimum-security standards and are compliant with basic requirements. They have foundational security practices implemented, such as regular patching, basic access controls, and some level of incident response. However, their cybersecurity posture remains rudimentary, with room for improvement in key areas such as advanced threat detection.
70 - 79%	Entities in this range have made significant strides in their cybersecurity efforts, demonstrating a moderate level of maturity. They have implemented a broader range of security controls, such as multi-factor authentication (MFA), encryption, and more sophisticated monitoring. However, while they have addressed major security concerns, their processes and technologies may still lack optimization or full integration across the organization.
80 - 89%	Entities scoring in this range have achieved a strong level of security maturity. They have robust and well-integrated security controls, such as continuous monitoring, advanced threat detection, and comprehensive encryption policies. Their security posture is proactive, and they can effectively manage risks. However, there may still be opportunities for fine-tuning to reach maximum capability.
90 - 100%	At this level, entities exhibit comprehensive, proactive cybersecurity practices. They have fully integrated security controls across all areas, with real-time threat detection, advanced risk management, and regular assessments driving continuous improvement. These organizations stay ahead of emerging threats through adaptive security measures and maintain a strong culture of cybersecurity.

CONFIDENTIAL