Annual Security Summary Report on Self-Certification Compliance for Independent Entities

Government Code Section 11000 Agencies
Independent Boards, Commissions, &
Constitutional Entities

Table of Contents

Executive Summary

This Annual Security Summary Report (Report) is prepared by the California Department of Technology (CDT) pursuant to Government Code (GC) Section 11549.3(f)(4)(E). The Report provides an aggregate view of the security posture and compliance status of state agencies, defined under GC Section 11000, that are not under the direct authority of the Governor and are not required to comply with the information security, privacy, and reporting policies and standards developed by CDT under GC Section 11549.3(b) (GC Section 11000 entities). GC Section 11000 entities are required to annually certify with CDT their compliance under GC Section 11549.3(f), which includes: (1) adoption of information security and privacy policies, standards, and procedures that adhere to National Institute of Standards and Technology (NIST) and Federal Information Processing Standards (FIPS); (2) performance of an independent security assessment (ISA) every two years that assesses the adopted information security and privacy policies, standards, and procedures; and (3) submission of a plan of action and milestones (POAM).

Submissions are aggregated to create the Report and provide a comprehensive overview of the cyber resiliency and maturity of GC Section 11000 entities. The consolidated view supports statewide understanding of cybersecurity maturity and highlights systemic trends. It also identifies areas where security practices are strong as well as opportunities for GC Section 11000 entities to improve.

This year marks the third Annual Security Summary Report and continues the trajectory established in prior years. Building on earlier insights, this Report focuses on the security trends emerging across GC Section 11000 entities and provides recommendations aimed at strengthening cyber resilience statewide.

Key Findings

GC Section 11000 Entities Identified	State Information Management Manual (SIMM) 5330-F Certifications Received	ISAs Received	POAMs Received
24	15	11	12

GC 11000 Entities' ISA Summary

- Inconsistent governance, asset hygiene, and vulnerability management continue to hinder cybersecurity maturity.
- Continued use of unsupported or legacy systems reflects weaknesses in system lifecycle management.
- Phishing risk remains high due to weak password practices.

GC 11000 Entities' POAMs Summary

- Planning remains the most frequently cited high-severity control gap, reflecting ongoing deficiencies in security planning and risk management documentation.
- Significant deficiencies persist in access control, authorization, monitoring, and configuration management, limiting consistent policy enforcement and secure baseline maintenance.
- Remediation timelines show slight deterioration and remain excessively long, indicating insufficient prioritization of known risks.

Background

In 2023, Governor Newsom signed AB 127 (Committee on Budget) – State Government, which requires every Independent & Constitutional (GC 11000) entity to certify by February 1 of each year their compliance with all cybersecurity policies, standards, and procedures. AB 127 [2023] also authorized CDT to receive and review the certifications and make a summary report available annually to the Legislature.

Outreach

CDT notified entity heads, Chief Information Officers (CIOs), and Information Security Officer (ISOs) of GC Section 11000 entities to underscore the significance of the statute and compliance reporting requirements. This initiative was part of CDT's strategic effort to ensure our expertise and guidance were readily accessible to support GC Section 11000 entities in meeting their compliance objectives.

CDT identified 24 state entities as GC Section 11000 entities (see Appendix A) and notified them about the GC Section 11549.3 and its certification and compliance requirements, These requirements include[1]:

- Adopting and implementing information security and privacy policies, standards, and procedures that adhere to:
    - NIST Special Publication 800-53 Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations, and its successor publications.
    - 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.
- Performing a comprehensive ISA every two years that assesses the adopted information security and privacy policies, standards, and procedures.
- Filing a self-certification of compliance annually that includes the ISA findings and POAM in accordance with SIMM section 5330-F, Information Security and Privacy Program Compliance Certification for Independents and Constitutionals.

Compliance

For the purposes of this Report, submissions to CDT were due no later than February 1, 2026. Documentation received after this date was not considered for this year's Report. GC Section 11000 entities that fail to meet this deadline will be identified as noncompliant. This approach ensures transparency while supporting accurate, timely, and complete reporting in accordance with statutory requirements.

[1] Under GC Section 11549.3(f)(5), GC Section 11000 entities may alternatively comply with these requirements by annually submitting a declaration to the State Chief Information Security Officer by January 15 that they voluntarily and fully comply with the security and privacy requirements applicable to state entities that are under the direct authority of the Governor as described in GC Section 11549.3(b) and (c).

The compliance results are as follows:

- 15 of 24 5330-F Self Certifications were received.
- 11 of 24 ISAs were received.
- 12 of 24 POAMs were received.[2]

Independent Security Assessments

The ISAs are designed to evaluate the technical security capabilities of state entities, ensuring their resilience against cyber threats and real-world attacks. Through comprehensive penetration testing and technical assessments, these evaluations provide state entities with a clear understanding of their security posture, identifying vulnerabilities and potential points of exploitation within their environments. These assessments play a critical role in risk identification and mitigation strategies.

CDT has dedicated efforts to encourage collaboration among GC Section 11000 entities through targeted cybersecurity outreach programs. These initiatives are designed to improve the collection and quality of security data and metrics, enabling CDT to enhance its holistic understanding of the state's cybersecurity landscape to strengthen its overall cyber resiliency.

The list below outlines key areas from the ISA that were measured and analyzed due to their relatively high susceptibility to compromise:

- **ISA Score:** Provides a broader view of metrics not covered in this Report.
- **Total Active Directory Assets**: Provides the number of assets in active directory.
- **Unsupported Operating Systems:** Identifies legacy systems vulnerable to exploitation.
- **Unsupported Operating System Percentage:** Divides the unsupported operating system count by the Total Active Directory Assets count.
- **California Cybersecurity Vulnerability Metric (CCVM):** The vulnerability score metric derived from an average Risk-per-Host value. This is a comparative analysis of detected vulnerabilities against the industry standardized risk ratings system maintained in the NIST National Vulnerability Database.
- **Critical & High Vulnerabilities:** Counts the total critical and high vulnerabilities exposed. Multiple vulnerabilities on one asset can increase this metric.
- **Phishing Rate:** Percentage of staff who clicked on phishing emails compared to the total sample size.
- **Password Compromise Rate:** Percentage of staff who provided their credentials after clicking on a phishing link.

GC 11000 Entities' ISA Summary

Across the assessed GC Section 11000 entities, security programs demonstrate the presence of foundational controls, yet consistent gaps persist that inhibit GC Section 11000 entities from achieving a mature and resilient cybersecurity posture. The ISAs show that while many GC Section 11000 entities maintain reasonable baseline defenses, variability in governance, asset hygiene, and vulnerability management continue to drive uneven performance across the entities.
A recurring challenge is the ongoing reliance on unsupported or legacy operating systems.

[2] Two of the 24 entities self-attested their compliance to subdivisions (b) and (c) of GC Section 11549.3.

Although the prevalence varies, the existence of such assets, regardless of scale, signals structural lifecycle-management weaknesses. Unsupported systems cannot receive security updates, and when combined with high volumes of critical and high-severity vulnerabilities observed across many environments, they collectively amplify the attack surface. These patterns indicate that patching programs often struggle to keep pace with operational demands, leaving significant portions of the environment exposed for prolonged periods.

The ISAs also identified disparities in patch management maturity. Several GC Section 11000 entities demonstrate effective remediation processes, yet others retain elevated vulnerability backlogs despite sizeable scanning footprints. This inconsistency suggests that vulnerability identification is occurring, but remediation pipelines, prioritization methods, or resource allocations may not be aligned to reduce risk at the rate necessary to counter modern threats.

Human-centric security controls likewise require continued emphasis. Phishing susceptibility remains highly variable across GC Section 11000 entities, with some showing substantial risk exposure. Elevated click-through rates, coupled with weak password practices observed in pockets of the GC Section 11000 entities, point to a need for more frequent and targeted security awareness training. As threat actors increasingly rely on social engineering, strengthening workforce readiness is a critical component of operational resilience.

Overall, the aggregated ISA results indicate that while security fundamentals are in place, GC Section 11000 entities must accelerate efforts to modernize aging infrastructure, strengthen patching and vulnerability remediation processes, and cultivate a culture of security-minded behavior. Addressing these systemic gaps will reduce risk accumulation, improve incident prevention capability, and support the long-term integrity and reliability of state operations.

Plan of Action and Milestones

All state entities are entrusted with establishing an information security program to ensure the proper use and protection of State-owned and managed information assets. State entities are accountable for tracking and documenting security deficiencies and organizational cyber risks identified through ISAs, audits, and self-observations in a POAM.

POAMs are intended to document risks, potential threats, and vulnerabilities that could negatively impact the security or integrity of a system, network, or data that the state entity owns. These risks are identified by analyzing the current security measures, identifying potential threats, evaluating the likelihood of those threats, and assessing the potential damage they could cause if not addressed. The goal is to reduce the potential for unauthorized access, data breaches, loss of data integrity, and other security incidents.

Findings on the POAM are indexed around 20 different security-related categories, also known as "Security Controls," to protect the confidentiality, integrity, and availability of information assets, as identified in FIPS 200. Additionally, findings are labeled with a severity risk level to help prioritize the findings with a plan of action.

POAM security control categories include:

POAM Security Categories		
Access Control	Awareness & Training	Audit & Accountability
Assessment, Authorization & Monitoring	Configuration Management	Contingency Planning
Identification & Authentication	Incident Response	Maintenance
Media Protection	Physical & Environmental	Planning
Program Management	Personnel Security	PII Processing & Transparency
Risk Assessment	System & Services Acquisition	System & Communications
System & Information Integrity	Supply Chain Risk Management	

CDT received 12 POAM submissions from GC Section 11000 entities. The following findings are the results of a detailed examination of the data collected:

Top four security controls with the most findings	Top area of focus by severity rating
● Planning (109) ● Access Control (70) ● Configuration Management (61) ● Assessment, Authorization, and Monitoring (58)	● High: Planning (65) ● Moderate: Assessment, Authorization, and Monitoring (35) ● Low: System and Information Integrity (24) ● Very Low: Planning (14)

On average there are 9.0 moderate and 6.13 high findings this year, a significant reduction from last year's average of 22.1 moderate and 10.4 high findings. The median time to remediate (MTTR) has deteriorated slightly, increasing from 448 days to 459 days. This duration is far above acceptable thresholds for effective risk mitigation. To further strengthen remediation efforts, CDT continues to offer support to GC Section 11000 entities to prioritize risk and promote timely closure of findings, reinforcing sustainable vulnerability management practices.

GC Section 11000 Entities' POAM Summary

The POAM submissions for the current reporting cycle highlight several thematic areas where GC Section 11000 entities experience challenges. **Planning** was the most frequently cited control area, indicating persistent gaps in foundational governance activities such as developing, maintaining, and updating security plans and risk management documentation. This trend is further reinforced by planning's prominence among high-severity findings, suggesting that strategic and programmatic deficiencies continue to translate into elevated organizational risk.

Access Control, **Configuration Management, and Assessment/Authorization/Monitoring** follow closely as additional areas of concern. These findings point to weaknesses in day-to-day operational security, such as inconsistent enforcement of access policies, challenges maintaining secure configurations across complex environments, and limited oversight of system authorizations. Collectively, these patterns suggest that while GC Section 11000 entities may have baseline controls in place, they continue to struggle with implementing and sustaining

them in a consistent, measurable, and risk-responsive manner. This year's aggregate counts[3] of moderate and high findings are lower than the previous cycles by 59.3% and 41.1% respectively.

The data suggests that risk identification and documentation practices are weak, which reduce visibility, and findings remain unresolved, lowering security posture. The MMTR high-risk and moderate risk findings show 12% and 10% increases, respectively, indicating that known issues are not being addressed with the urgency required to meaningfully reduce risk exposure. Moving forward, strengthening governance processes, improving the rigor of risk identification, and accelerating remediation timelines will be essential for advancing statewide security maturity.

Conclusion

This year's Report highlights incremental progress in several areas, such as evidence of closing moderate and high risks identified in the POAM, emphasizing the continued need for continuous reporting of independent entity risk identification, governance, and remediation practices. The insights gained from the POAM submissions and ISA trends provide a clearer picture of where GC Section 11000 entities are advancing and where foundational security processes require renewed attention. As GC Section 11000 entities work to modernize legacy controls, improve visibility into vulnerabilities, and reduce remediation timelines, coordinated statewide efforts remain essential for sustaining long-term improvements in cybersecurity maturity.

CDT remains committed to supporting GC Section 11000 entities through targeted outreach, advisory engagement, and capacity-building efforts designed to enhance both programmatic and operational security. By continuing to refine risk management processes and address systemic gaps identified in this report, GC Section 11000 entities can strengthen their resilience and better safeguard the systems and data entrusted to them. CDT will continue to build on this year's findings, ensuring ongoing visibility into statewide trends and driving collaborative progress across the enterprise.

[3] Contextually, remediation metrics should be interpreted in context, as higher-risk findings are weighted more heavily and the closure of individual POAM items does not contribute equally to overall risk reduction. Progress should be evaluated based on the severity and potential impact of risks addressed, rather than the quantity of items closed.

Appendix A – GC 11000 Entity Responses

The following table provides a summarized matrix of submissions received by CDT by the December administrative deadline.

R = Received, SD = Self-Declared Compliance to subdivision (b) and (c) of GC Section 11549.3.

Org Code	Entity Name	POAM	POAM Cover Page	5330-F Compliance	ISA
552	Office of the Inspector General	R	R	R	R
750	Office of the Lieutenant Governor	-	-	-	-
820	Office of the Attorney General - Department of Justice	-	-	-	-
840	State Controller's Office	-	-	R	-
845	Department of Insurance	R	R	R	R
850	California State Lottery	SD	SD	R	SD
855	California Gambling Control Commission	R	R	R	-
860	State Board of Equalization	R	R	R	R
870	Office of Tax Appeals	R	R	R	R
890	Office of the Secretary of State	-	-	-	-
950	State Treasurer's Office (STO)	-	-	-	-
1703	California Privacy Protection Agency	R	R	R	R
4800	California Health Benefit Exchange (Covered CA)	SD	SD	R	SD
6100	Department of Education	-	-	-	R
6125	Education Audit Appeals Panel	-	-	-	-
6255	California State Summer School for the Arts	R	R	R	-
8120	Commission on Peace Officer Standards and Training (POST)	R	R	R	R
8385	California Citizens Compensation Commission	R	R	R	R
8620	Fair Political Practices Commission	R	R	R	R
8660	Public Utilities Commission	R	R	R	R
8780	Milton Marks "Little Hoover" Comm. on California State Gov. Organization & Economy	-	-	-	-
8830	California Law Revision Commission	-	-	-	-
8855	California State Auditor's Office	-	-	-	-
8885	Commission on State Mandates	R	R	R	R

The following table below provides the reasoning for the use-cases associated with fully submitted, partially submitted, and non-submitted items.

Org Code	Entity Name	Reason Given for Reporting Status
552	Office of the Inspector General	Fully Reported
750	Office of the Lieutenant Governor	No Response/Declined to report or indicate self-certification.
820	Office of the Attorney General - Department of Justice	No Response/Declined to report or indicate self-certification.
840	State Controller's Office	Only SIMM 5330-F was submitted. Declined to report POAM and POAM Cover Sheet. No ISA was conducted.
845	Department of Insurance	Fully Reported.
850	California State Lottery	Stated an alternative reporting process to the Legislature through a self-certification that they met all mandated compliance requirements.
855	California Gambling Control Commission	Fully Reported; however, did not have an ISA to submit.
860	State Board of Equalization	Fully Reported
870	Office of Tax Appeals	Fully Reported
890	Office of the Secretary of State	No Response/Declined to report or indicate self-certification.
950	State Treasurer's Office (STO)	No Response/Declined to report or indicate self-certification.
1703	California Privacy Protection Agency	Fully Reported
4800	California Health Benefit Exchange (Covered CA)	Stated an alternative reporting process to the Legislature through a self-certification that they met all mandated compliance requirements.
6100	Department of Education	Submitted an ISA. Declined to report certifications and POAM.
6125	Education Audit Appeals Panel	No Response/Declined to report or indicate self-certification.
6255	California State Summer School for the Arts	Fully Reported; however, did not have an ISA to submit.
8120	Commission on Peace Officer Standards and Training (POST)	Fully Reported
8385	California Citizens Compensation Commission	Fully Reported
8620	Fair Political Practices Commission	Fully Reported
8660	Public Utilities Commission	Fully Reported

8780	Milton Marks "Little Hoover" Comm. on California State Gov. Organization & Economy	No Response/Declined to report or indicate self-certification.
8830	California Law Revision Commission	No Response/Declined to report or indicate self-certification.
8855	California State Auditor's Office	No Response/Declined to report or indicate self-certification.
8885	Commission on State Mandates	Fully Reported

The following entities have failed to **fully**[4] meet their compliance reporting requirements under Government Code Section 11549.3 in the last two consecutive years.

Org Code	Entity Name	2024	2025
0750	Office of the Lieutenant Governor	-	-
0820	Office of the Attorney General - Department of Justice	-	-
0840	State Controller's Office	-	-
950	State Treasurer's Office (STO)	-	-
6125	Education Audit Appeals Panel	-	-
8780	Milton Marks "Little Hoover" Comm. on California State Gov. Organization & Economy	-	-
8830	California Law Revision Commission	-	-
8855	California State Auditor's Office	-	-

[4] Partial compliance is not considered full compliance.