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

Government Code §11000 Agencies

Independent Boards, Commissions, & Constitutional Entities

Table of Contents

Table of Contents 1
Executive Summary 2
Background 3
Outreach 3
Compliance 3
Independent Security Assessment 4
    GC 11000 Entities' ISA Summary 4
Plan of Action and Milestones 6
    GC 11000 Entities' POAM Summary 7
Conclusion 8
Appendix A – GC 11000 Entity Responses 9

Executive Summary

The Annual Security Summary Report (Report), prepared by California Department of Technology (CDT) in accordance with Government Code (GC) §11549.3(f)(4)(E), provides an overview of security compliance across state agencies as defined by GC §11000. Independently elected boards, commissions, and other GC §11000 entities are required to submit independent security assessments, self-certifications, and a list of non-compliant security gaps required by the National Institute of Standards and Technology (NIST) Special Publication 800-53 and Federal Information Processing Standards (FIPS) 199 and 200, to CDT. While CDT is authorized to analyze these submissions and offer recommendations, it does not have enforcement authority over GC §11000 entities. These submissions contribute to individual security risk profiles, which are then aggregated to create the Report, offering a comprehensive view of cyber resiliency and maturity across all GC §11000 entities.

The Report identifies security trends among GC §11000 entities, highlighting strengths as well as areas for improvement. Two key areas of concern - Configuration Management and Access Control - account for the majority of identified risks. To address these vulnerabilities, GC §11000 entities are encouraged to adopt the NIST Cybersecurity Framework and implement appropriate tools, technologies, and processes to mitigate risks based on NIST remediation measures. Additionally, CDT encourages GC §11000 entities to initiate consultations with the CDT Advisory Services for guidance on best practices and available remediation resources to help expedite the resolution of security findings in these areas.

Published annually, the Report supports legislative committees and the Legislative Analyst's Office in their oversight and budgetary responsibilities. This is the second edition of the Report, and this year's Report employs a more refined vetting process to focus specifically on entities that fall under GC §11000. As a result, the scope has been adjusted, and some entities are no longer included.

Background

In 2023, Governor Newsom signed Assembly Bill (AB) 127 (Committee on Budget) – State Government, which amended GC §11549.3 to require, among other things, that every GC §11000 entity's certification of compliance with all policies, standards, and procedures adopted pursuant to GC §11549.3(f) be completed and sent to CDT's Office of Information Security (OIS) on a form developed by OIS. AB 127 also required CDT OIS to review the certifications and make an annual summary report available every year, to the appropriate legislative committees and the Legislative Analyst's Office on behalf of the entities to further their oversight and budgetary responsibilities.

Outreach

A concerted outreach was conducted notifying GC §11000 entity heads, Chief Information Officers, and Information Security Officers, to underscore the significance of the change in statute and compliance reporting requirements. This initiative was part of CDT's strategic effort to ensure its expertise and guidance were readily accessible to support GC §11000 entities in meeting their compliance objectives.

Twenty-six (26) entities were notified about the amendment to GC §11549.3, through various outreach programs, stating that every state agency, as defined in GC Section §11000 and not subject to GC 11549.3(b)(see Appendix A), will have reporting and compliance requirements that include:

- Adopting and implementing information security and privacy policies, standards, and procedures that adhere to requirements GC §11549.3 (f)(1)(A).
- Performing a comprehensive independent security assessment (ISA) every two years pursuant GC §11549.3 (f)(1)(B).
- Filing a self-certification of compliance annually pursuant GC §11549.3 (f)(4)(A).
- Filing a Plan of Action and Milestones (POAM) to CDT annually pursuant GC §11549.3 (f)(4)(A).
- Filing the results of their independent security assessments pursuant GC §11549.3 (d).

Compliance

The 2024 compliance results for GC §11000 entities choosing to report to CDT OIS are as follows:

- Twelve (12) of twenty-six (26) ISAs were received.
- Fourteen (14) of twenty-six (26) self-certifications were received.
- Sixteen (16) of twenty-six (26) POAMs were received.
- One (1) of the twenty-six (26) GC §11000 entities successfully self-certified its compliance with subdivisions (b) and (c) of GC §11549.3 and was therefore exempt from submitting additional documentation.

Independent Security Assessment

The ISA are designed to evaluate the technical security capabilities of GC §11000 entities, ensuring their resilience against cyber threats and real-world attacks. Through comprehensive penetration testing and technical assessments, these evaluations provide GC §11000 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 §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 AD Assets**: Provides the number of assets in active directory (AD).
- **Unsupported Operating Systems:** Identifies legacy systems vulnerable to exploitation.
- **Unsupported OS %:** Divides the unsupported operating system count by the Total AD Asset count.
- **Critical & High Vulnerabilities:** Counts the total critical and high vulnerabilities exposed. Multiple vulnerabilities on one asset can increase this metric, while the average per-host weighted vulnerability score (CCVM) Patching Score measures vulnerabilities per asset.
- **CCVM Patching Score:** Shows an asset-level view of vulnerabilities. The CCVM measures vulnerabilities by asset rather than in total.
- **Phishing Rate:** Percent of staff who clicked on phishing emails compared to the total sample size.
- **Password Compromise Rate:** Percent of staff who provided their credentials after clicking on a phishing link.

GC 11000 Entities' ISA Summary

While foundational security mechanisms are in place, additional efforts are necessary to advance beyond baseline cybersecurity compliance. A strategic transition away from legacy assets remains imperative, as unsupported systems cannot be patched, posing inherent security risks. Unpatched vulnerabilities undermine the effectiveness of patch management programs, leaving GC §11000 entities exposed to potential threats.

Additionally, it was determined that GC §11000 entities require an enhanced security awareness and training program, as staff were found to be highly susceptible. Moreover, the inherent nature of high-profile personnel further increases the likelihood of phishing attacks. Addressing this challenge is essential to fostering a resilient cybersecurity culture.

The ISA Scores were aggregated resulting in an overall score that falls slightly below the state average. The convergence of unsupported operating systems, persistent vulnerabilities, and inconsistent patch management places GC §11000 entities at heightened risk of cyber

threats. Proactively mitigating these risks is essential to safeguarding operational integrity, maintaining public trust, and preventing financial and reputational damage.

By modernizing legacy assets, GC §11000 entities can significantly enhance their security posture, reduce vulnerability exposure, and bolster privacy protection - ensuring a more resilient and secure operational environment.

Plan of Action and Milestones

All state entities are entrusted with establishing an information security program to ensure the proper use and protection of California State-owned information assets. GC §11000 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 GC §11000 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 twenty (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		

CDT received 16 POAM submissions from GC §11000 entities during the January 2025 reporting cycle. The following findings are the results of a detailed examination of the data collected:

Top 4 security controls with the most findings	Top area of focus by severity rating
• Configuration Management (103) • Access Control (102) • Authentication Monitoring (88) • System Integrity (73)	• High: Risk Assessment (31) • Medium: Access Control (49) • Low: Access Control (33) • Very Low: Contingency Planning (11)

There are an average of 22.1 moderate and 10.4 high findings for each GC §11000 reporting entity, reflecting an increase compared to last year's report, which recorded an average of 11.36 moderate and 4.71 high findings. This trend suggests an improvement in risk identification processes.

Additionally, the median time to remediate (MTTR) a finding has decreased to 448 days (approximately 1.25 years), down from 494 days (about 1.5 years) last year, indicating a modest improvement in remediation speed. To further accelerate this progress, the CDT's Advisory Services team plans to engage with these GC §11000 entities and support efforts to reduce MTTR.

GC §11000 Entities' POAM Summary

GC §11000 entities signaled an opportunity for growth primarily in the Configuration Management security control. The Configuration Management security control provides a structured process that involves managing changes to systems, including software, hardware, and documentation.

GC §11000 entities showed a secondary area of improvement in Access Control. Access Control is the third highest focal point for the State of California and focuses on implementing policies and procedures that ensure only authorized individuals, systems, or processes can access specific resources, thus securing the organization's systems and data.

By refining approaches to Configuration Management and Access Controls, GC §11000 entities can significantly improve risk management and achieve stronger security and privacy capabilities that reduce the risk of breaches. This addresses potential weaknesses and demonstrates a commitment to cyber resilience, safeguarding sensitive information, and upholding data integrity and confidentiality against cyber threats and compliance issues.

Conclusion

This Report sets a solid foundation for identifying and addressing security vulnerabilities for the greater good of California. It is a positive step towards coordinating risk management efforts, enhancing security and privacy measures, and aligning with state goals while reducing the State's exposure to threats and breaches.

CDT looks forward to partnering with GC §11000 entities to improve the State's overall cybersecurity maturity and capabilities. Future Reports will continue to be made available annually. CDT is committed to providing the assistance necessary to help GC §11000 entities meet their compliance requirements effectively with additional outreach efforts throughout the year.

Appendix A – GC 11000 Entity Responses

R = Received, NR = Not Received, SC = Self Certified Compliance to subdivision (b) and (c) of GC §11549.3

Org Code	Entity Name	POAM	POAM Cert	Compliance Cert	ISA
0840	State Controller's Office	SC	SC	R	SC
0750	Office of the Lieutenant Governor	NR	NR	NR	NR
0820	Department of Justice	NR	NR	NR	NR
0850	California State Lottery	NR	NR	NR	NR
0950	State Treasurer's Office	NR	NR	NR	NR
4800	California Health Benefit Exchange	NR	NR	NR	NR
6125	Education Audit Appeals Panel	NR	NR	NR	NR
6255	California State Summer School for the Arts	NR	NR	NR	NR
8420	State Compensation Insurance Fund	NR	NR	NR	NR
8780	Little Hoover Commission	NR	NR	NR	NR
0870	Office of Tax Appeals	R	R	NR	R
8385	California Citizens Compensation Commission	R	R	R	R
0845	California Department of Insurance	R	R	R	R
0860	Board of Equalization	R	R	R	R
1703	California Privacy Protection Agency	R	R	R	R
6100	Department of Education	R	R	R	R
8120	Commission on Peace Officer Standards & Training	R	R	R	R
8620	Fair Political Practices Commission	R	R	R	R
8660	California Public Utilities Commission	R	R	R	R
8885	Commission on State Mandates	R	R	R	R
0552	Office of the Inspector General	R	R	NR	R
8820	Commission on the Status of Women & Girls	R	R	R	R
0855	California Gambling Control Commission	R	R	R	NR
0890	Secretary of State	R	R	R	NR
8855	California State Auditor	R	NR	R	NR
8830	California Law Revision Commission	R	R	NR	NR