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

Government Code 11000 Agencies

Independent Boards, Commissions, & Constitutional Entities

Office of Information Security
California Department of Technology

Table of Contents

Table of Contents 1
Executive Summary 2
Background 3
Outreach 3
Compliance 3
Information Security Assessment 4
GC 11000 Entities' ISA Summary 4
Plan of Action and Milestones 5
GC 11000 Entities' POAM Summary 6
Conclusion 7
Appendix A – GC 11000 Entity Responses 8

Executive Summary

The Annual Security Summary Report, pursuant to Government Code (GC) 11549.3, is prepared by the California Department of Technology (CDT) and details the current rate of security compliance and status of Agencies, as defined by GC 11000, collectively. Independently elected Boards, Commissions, and independent entities being defined as GC 11000 entities are now required to submit annual security assessments, self-certifications, incident reports, and a list of identified security risks and vulnerabilities throughout their organization to the President pro-Tempore of the Senate and the Speaker of the Assembly or as an option authorize the CDT to receive compliance documentations. The CDT is authorized to provide recommendations and analysis of the documentation received from entities who choose to report. The CDT has no authority to enforce compliance for GC 11000 entities. These submissions are used to create individual security risk profiles for each entity, which are then aggregated to create the Annual Security Summary Report and provide a comprehensive overview of the cyber resiliency and maturity of all the entities.

The Annual Security Summary Report aims to identify and correlate security trends among GC 11000 entities and identify areas of excellence and potential improvements as recommendations to consider. This report is made available May 1, 2024, and March 1 every year thereafter, to legislative committees and the Legislative Analyst's Office to further their oversight and budgetary responsibilities.

It is worth noting that this is the first Annual Security Summary Report highlighting security risk trends across the GC 11000 entities. While the sample size is small, due to limited participation, CDT continues to work with these entities to improve their participation and reporting.

Background

In 2023, Governor Newsom signed AB 127 (Committee on Budget) – State Government, which amended Government Code Section 11549.3 to require every GC 11000 entity, as described, to certify by February 1 annually, authorizing CDT to receive evidence of compliance with all policies, standards, and procedures adopted pursuant to GC 11549.3(f). AB 127 authorized CDT to review the certifications and make an annual summary report available by May 1, 2024, and by March 1 every year thereafter, 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 entity heads, CIOs, and ISOs, to underscore the significance of the change in statute and compliance reporting requirements. This initiative was part of CDT's strategic effort to ensure our expertise and guidance were readily accessible, supporting entities in meeting their compliance objectives.

Thirty-three entities were notified about the amendment to GC 11549.3, through various outreach programs, stating that every GC 11000 entity, as defined in GC Section 11000 (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 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 compliance results for entities choosing to report to CDT are as follows:

- Two of 33 ISAs were received.
- Eleven of 33 self-certifications were received.
- Fourteen of 33 POAMs were received; two of the fourteen POAMs were only partially complete.

Information Security Assessment

GC 11000 Entities' ISA Summary

Given the limited number of GC 11000 entities choosing to submit ISA's, CDT was unable to provide a meaningful analysis or comparison to statewide trends. Within the scope of CDT's authority, to ensure robust and thorough evaluations going forward, CDT plans to increase its outreach efforts to further encourage GC 11000 entities take advantage of the California Department of Military's services for conducting ISAs and reporting the results to CDT. This will help streamline the process and enhance the quality of security data and metrics enabling CDT to improve its understanding of the state's cybersecurity landscape.

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. 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 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 different security-related categories, also known as "Security Controls," to protect the confidentiality, integrity, and availability of information assets, as identified in the Federal Information Processing Standards (FIPS) Publication (PUB) 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 14 POAM submissions from GC 11000 entities during the January 2024 reporting cycle.

The following summarizes the results:

Top 4 security controls with the most findings	Top area of focus by severity rating
• Planning (52) • Access Control (44) • Configuration Management (26) • Risk Assessment (25)	• High: Planning (17) • Medium: Access Control (27) • Low: Planning (13) • Very Low: Access Control (4) & Awareness and Training (4)

On average, GC 11000 entities have 11.36 moderate and 4.71 high findings. Furthermore, the median time to remediate (MTTR) a finding is 494 days (about 1.5 years). Given this MTTR, the CDT's Advisory Services team plans to engage these entities to assist in efforts to drive this timeline down.

GC 11000 Entities' POAM Summary

GC 11000 entities signaled an opportunity for growth primarily in the Planning security control. The Planning security control provides a structured approach that assists organizations with formulating, documenting, and enacting their security and privacy protocols.

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 Planning 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 initial Annual Security Summary 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 be made available annually by March 1st. CDT is committed to providing the assistance necessary to help entities meet their compliance requirements effectively with additional outreach efforts throughout the year.

Appendix A – GC 11000 Entity Responses

R = Received, NR = Not Received, P = Partially Complete

Org Code	Entity Name	SIMM 5330-F	ISA	POAM
0552	Office of the Inspector General	R	R	R
0845	California Department of Insurance	R	NR	R
6120	California State Library	R	NR	R
6980	California Student Aid Commission	R	NR	R
8120	Commission on Peace Officer Standards and Training	R	NR	R
8260	California Arts Council	R	NR	R
8660	California Public Utilities Commission	R	NR	R
8885	State of California Commission on State Mandates	R	NR	R
6100-6110	California Department of Education	R	NR	R
6360	Commission on Teacher Credentialing	NR	NR	R
8620	California Fair Political Practices Commission	NR	NR	R
0820	Department of Justice (Office of the Attorney General)	R	NR	R
8140	Office of the State Public Defender	R	NR	NR
0750	Office of the Lieutenant Governor	NR	NR	NR
0840	State Controller's Office	NR	NR	NR
0850	California State Lottery Commission	NR	NR	NR
0855	California Gambling Control Commission	NR	NR	NR
0860	California State Board of Equalization	NR	NR	P
0890	California Secretary of State	NR	NR	NR
0950	State Treasurer's Office	NR	NR	NR
4250	First 5 California (Children and Families Commission)	NR	NR	NR
4800	California Health Benefit Exchange (Covered California)	NR	NR	NR
6125	Education Audit Appeals Panel	NR	NR	NR
6255	California State Summer School for the Arts	NR	NR	NR
6870	California Community Colleges Chancellor's Office	NR	NR	P
8385	California Citizens Compensation Commission	NR	NR	NR
8420	State Compensation Insurance Fund	NR	NR	NR
8560	California Exposition & State Fair	NR	NR	NR
8780	Little Hoover Commission	NR	NR	NR
8820	California Commission on the Status of Women and Girls	NR	NR	NR
8825	Commission on Asian & Pacific Islanders American Affairs	NR	NR	NR
8830	California Law Revision Commission	NR	NR	NR
8855	California State Auditor	NR	R	NR