

---

---

**State of California**  
**California Department of Technology**  
**Office of Information Security**  
**Information Security and**  
**Privacy Program Compliance Certification**  
**for Independents and Constitutionals**  
**SIMM 5330-F**  
**January 2024**

---

---

## REVISION HISTORY

| REVISION        | DATE OF RELEASE | OWNER                                     | SUMMARY OF CHANGES  |
|-----------------|-----------------|---|---|
| Initial Release | October 2023    | California Office of Information Security |   |
| 1.2             | January 2024    | California Office of Information Security | <b>MINOR UPDATE:</b> Requesting ISO and CIO contact information and a missing option for attachments. |

**TO:** Office of Information Security,  
California Department of Technology  
Attn: Security Compliance Reporting  
P.O. Box 1810, Mail Stop Y- 01  
Rancho Cordova, CA 95741

**DATE:**

**AGENCY NAME:**

**ORG CODE:**

(As identified in the [Uniform Codes Manual](#))

Separate compliance forms are required for ALL state agencies regardless if they meet the criteria for a Host/Hosted relationship.

**SUBJECT: Information Security and Privacy Program Compliance Certification**

As specified in [Government Code Section 11549.3](#) "(f)(4)(A) Every state agency described in paragraph (1) shall certify, on a form developed pursuant to subparagraph (C), by February 1 annually, to the office that the agency is in compliance with all policies, standards, and procedures adopted pursuant to this subdivision. The certification shall include a plan of action and milestones."

**As the state agency head or the acting state agency head, I certify:**

- I have ensured a standing governance body has been established to direct the development and ongoing maintenance of my agency's information security and privacy programs, and the management of identified risks.
- I meet with and am fully briefed by our agency's standing governance body on the status of the agency's information security and privacy programs compliance, including all agency risks identified through:
  - Information Security Program Audits,
  - Independent Security Assessments,
  - Risk Register & Plan of Action and Milestones (POAM) (SIMM 5305-C) reporting, and
  - Any other enterprise risk assessment or privacy impact assessment processes conducted by or for my agency.
- I have prioritized and directed the completion of the required privacy program compliance reporting and associated risk response activities for each of our agency's information technology systems to ensure risk and liability is brought to an acceptable level aligned with the organization's risk appetite.

- Our agency's information security privacy policies, standards and procedures are compliant with the following standards and that I and other senior management recognize all deficiencies that must be addressed:
  - (i) The 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.
  - (ii) Federal Information Processing Standards (FIPS) 199 Standards for Security Categorization of Federal Information and Information Systems, and its successor publications.
  - (iii) Federal Information Processing Standards (FIPS) 200 Minimum Security Requirements for Federal Information and Information Systems, and its successor publications.
- I fully understand the potential impacts of all risk findings not being addressed in an appropriate and timely manner.

**Attached as required is our agency's (select one):**

- Confidential POAM and Independent Security Assessment findings; or
- Confidential Independent Security Assessment findings only; or
- Confidential POAM only

**I plan or am actively engaged in the following services offered by CDT:**

- 24/7 Network Monitoring and Security Event and Vulnerability Notifications (SOCaaS)
- Active Threat Hunting and Scanning
- Forensic Investigation and Malware Analysis – Through the California Cybersecurity Integration Center (Cal-CSIC)
- Counseling and consultation with the Office of Information Security (OIS) Advisory Program, including the Virtual CISO program and Infusion Team.
- Incident Management through the California Compliance and Security Incident Reporting System (Cal-CSIRS)
- Organizational Risk Assessments with Security Risk Profiles and Maturity Metrics
- Information Security Program Audits (ISPA)

Independent Security Assessments (ISA) – Conducted through the California Military Department (CMD)

**Designated Chief Information Officer (CIO) Contact Information:**

\_\_\_\_\_  
Name Telephone Number Email

**Designated Chief Information Security Officer (CISO) Contact Information:**

\_\_\_\_\_  
Name Telephone Number Email

**Signature of the Secretary/Director (or equivalent agency head):**

\_\_\_\_\_  
Name Signature Date

**Enclosure(s):** Confidential High Risk Findings Report (if applicable) and POAM

**Securely send this entire form and all enclosures to the OIS using the Secure Automated File Exchange (SAFE) system.**  
**Contact OIS for assistance and/or instructions on access to the SAFE system at (916) 445-5239 or at [Security@state.ca.gov](mailto:Security@state.ca.gov).**