



California
DEPARTMENT OF TECHNOLOGY

Policy/Guidelines Update

DATE ISSUED: January 2018

TO: Chief Information Officers (CIO), Information Security Officers (ISO), Agency Chief Information Officers (AIO), Agency Information Security Officers (AISO)

SUBJECT: Updated Information Security Reporting Documents

REFERENCES: Statewide Information Management Manual (SIMM) Sections: 5330-A, 5330-B, 5330-C and Cal-CSIRS Designee Request Forms State Administrative Manual (SAM) Section 5330.2

Background:

The California Department of Technology's (CDT) Office of Information Security (OIS) has updated requirements to support compliance and security incident reporting. These updates better align compliance reporting and support implementation of the California Compliance and Security Incident Reporting System (Cal-CSIRS) risk reporting module state entities will use to complete their self-assessments for mission critical information systems.

Purpose:

The purpose of this policy/guidelines update is to announce changes to the following information security compliance sections, along with mandatory reporting documents:

- Revised SIMM Section 5330-A Annual Designation Letter and SIMM Section 5330-B Information Security and Privacy Program Compliance Certification to support the Cal-CSIRS Risk Reporting module implementation, eliminate the no-change certification option for Technology Recovery Plan (TRP) submissions, identify parent-child entity relationships in annual Designation Letter submissions, and provide additional instruction and clarity for all reporting requirements. Agencies/state entities must submit SIMM Sections 5330-A and 5330-B, along with mandatory supporting documents, to the OIS by April 30, 2018. Please note, there are no changes to the TRP monthly submissions schedule for 2018.
- Effective January 2019, SIMM Section 5330-C Security Compliance Reporting Schedule replaces the previous schedule outlined in State Administrative Manual (SAM) Section 5330.2. This new section provides reporting due dates

for all required information security compliance documents, along with mandatory supporting documents.

- Revised SAM Section 5330.2 Compliance Reporting to reflect changes to information security reporting requirements.
- General changes have been made to the following SIMM Sections, FAQs and Cal-CSIRS access request forms to align with report requirement changes referenced above.
 - SIMM 5305-A: Information Security Program Management Standard
 - SIMM 5305-B: Plan of Action and Milestones Instructions
 - SIMM 5305-C: Plan of Action and Milestones Worksheet
 - POAM FAQ: Plan of Action and Milestones Frequently Asked Questions (FAQ's)
 - SIMM 5310-A: Privacy Statement and Notices Standard
 - SIMM 5310-B: Privacy Individual Access Standard
 - SIMM 5325-A: Technology Recovery Plan Instructions
 - SIMM 5325-B: Technology Recovery Program Certification
 - SIMM 5330-A: Designation Letter
 - SIMM 5330-B: Information Security and Privacy Program Compliance Certification
 - SIMM 5330-C: Security Compliance Reporting Schedule
 - Cal-CSIRS Designee Request (Risk Reporting Tool)
 - SIMM 5340-A: Incident Reporting and Response Instructions
 - SIMM 5340-C: Requirements to Respond to Incidents Involving a Breach of Personal Information
 - Cal-CSIRS Designee Request (Incident Management)
 - CAL-CSIRS Frequently Asked Questions (FAQ)
 - SIMM 5360-A: Telework and Remote Access Security Standard
 - SIMM 5360-B: Remote Access Agreement

The Statewide Information Management Manual (SIMM) is available on the Department of Technology's website located at: <https://cdt.ca.gov/policy/simm/>. The State Administrative Manual (SAM) is available on the Department of General Services website located at: <http://sam.dgs.ca.gov/>.

Questions regarding this announcement should be directed to the CDT Office of Information Security at: security@state.ca.gov.