COMPLIANCE REPORTING **5330.2**
(Revised 01/2018)

Policy: Each state entity shall comply with the following reporting requirements:

1. **Designation Letter (SIMM 5330-A)** – Annual submissions are due to the Office of Information Security (OIS) on the last business day of the state entity's scheduled reporting month, as outlined in the Information Security Compliance Reporting Schedule (SIMM 5330-C). The state entity head shall designate the Chief Information Officer (CIO), Information Security Officer (ISO), Technology Recovery Coordinator and Privacy Officer/Coordinator, along with their back-up designees, using SIMM 5330-A. Upon the designation of a new CIO, ISO, Technology Recovery Coordinator, and a Privacy Officer/Coordinator, the state entity must submit an updated SIMM 5330-A to OIS within ten (10) business days.
2. **Information Security and Privacy Program Compliance Certification (SIMM 5330-B)** – Annual submissions are due to OIS on the last business day of the state entity's scheduled reporting month, as outlined in SIMM 5330-C. The state entity head shall certify that the entity is in compliance with state policy governing information security, risk management and privacy program compliance by submitting the SIMM 5330-B.
3. **Technology Recovery Plan (TRP) and Technology Recovery Program Compliance Certification (SIMM 5325-B)** – Each year the state entity head shall submit a copy of its TRP, along with the SIMM 5325-B to OIS by the last business day of the state entity's scheduled reporting month, as outlined in SIMM 5330-C. If the state entity employs the services of a data center, it must also provide the data center with a copy of its TRP or subset of the relevant recovery information from the state entity's TRP.
4. **Incident Report** – Incidents must be immediately reported in accordance with SAM Sections 5340-5340.4 requirements through the California Compliance and Security Incident Reporting System (Cal-CSIRS). The OIS may require, in conjunction with its assessment of the incident, that the state entity provide additional information.

Program deficiencies identified through compliance certification reporting, risk assessments, audits, incidents or oversight reviews also require the submission of a Plan of Action and Milestones Worksheet (POAM) (SIMM 5305-C). State entities shall follow the standardized POAM Instructions (SIMM 5305-B) when completing SIMM 5305-C. Unless otherwise directed, each state entity shall, at a minimum, provide quarterly updates on progress toward completion of the plans.

Quarterly submissions are due on the last business day of the following months; January, April, July and October.

(Continued)

(Continued)
COMPLIANCE REPORTING **5330.2 (Cont.)**
(Revised 01/2018)

Implementation Controls: Designation Letter (SIMM 5330-A); Information Security and Privacy Program Compliance Certification (SIMM 5330-B); Information Security Compliance Reporting Schedule (SIMM 5330-C); Technology Recovery Program Compliance Certification (SIMM 5325-B); Information Security Incident Report (SIMM 5340-B); and Plan of Action and Milestones Instructions and Worksheet (SIMM 5305-B and SIMM 5305-C).