

SAM – INFORMATION SECURITY
(Office of Information Security)

COMPLIANCE REPORTING
(Revised 6/2016)

5330.2

Policy: Each state entity shall comply with the following reporting requirements as directed by the CISO:

1. Designation Letter – By January 31 of each year, and as designee changes occur, the state entity head shall designate an ISO, Technology Recovery Coordinator and Privacy Officer/Coordinator using the Designation Letter ([SIMM 5330-A](#)). Upon the designation of a new ISO, Disaster Recovery Coordinator, and/or Privacy Program Coordinator, the state entity must submit an updated Designation Letter to the CISO within ten (10) business days using the Designation Letter ([SIMM 5330-A](#)).
2. Risk Management and Privacy Program Compliance Certification – By January 31 of each year, 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 Risk Management and Privacy Program Compliance Certification ([SIMM 5330-B](#)).
3. Technology Recovery Plan – Each year the state entity head shall submit a copy of its Technology Recovery Plan (TRP) with the Technology Recovery Program Compliance Certification ([SIMM 5325-B](#)) to the CISO by the due date outlined in the Technology Recovery Plan Submission Schedule. 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. The CISO 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 (POAM). State entities shall use the standardized POAM reporting instruction and tool ([SIMM 5305-B and SIMM 5305-C](#), respectively).

Implementation Controls: Designation Letter ([SIMM 5330-A](#)); Risk Management and Privacy Program Compliance Certification ([SIMM 5330-B](#)); Technology Recovery Program Compliance Certification ([SIMM 5325-B](#)); Information Security Incident Report ([SIMM 5340-B](#)); and Plan of Action and Milestones ([SIMM 5305-B and SIMM 5305-C](#)).