# SAM – INFORMATION SECURITY

**(Office of Information Security)**

**VULNERABILITY AND THREAT MANAGEMENT 5345**

(Revised 01/21)

**Introduction:** Threats and vulnerabilities provide the primary inputs to the state entity’s risk assessment process.

**Policy:** Each state entity shall continuously identify and remediate vulnerabilities before they can be exploited. Vulnerability and threat management include, but not limited to, the following:

1. Strategic placement of scanning tools to continuously assess all information technology assets;
2. Implementation of appropriate scan schedules, based on asset criticality;
3. Communication of vulnerability information to system owners or other individuals responsible for remediation;
4. Dissemination of timely threat advisories to system owners or other individuals responsible for remediation;
5. Consultation with system owners on mitigation strategies; and
6. Implementation of mitigation measures in accordance with the Vulnerability Management Standard (SIMM 5345-A).

**Implementation Controls:** NIST SP 800-53: [Risk Assessment (RA)](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf#page%3D307); [System and](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf#page%3D312) [Services Acquisition (SA)](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf#page%3D312); [System and Communication Protection (SC)](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf#page%3D340); Vulnerability Management Standard ([SIMM 5345-A](https://cdt.ca.gov/policy/simm/))