

**SAM – INFORMATION SECURITY**  
**(Office of Information Security)**

**VULNERABILITY AND THREAT MANAGEMENT**

5345

(Revised 12/13)

**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; and
5. Consultation with system owners on mitigation strategies.
6. Implementation of mitigation measures.

**Implementation Controls:** NIST SP 800-53: [Risk Assessment \(RA\)](#); [System and Services Acquisition \(SA\)](#); [System and Communication Protection \(SC\)](#)