INFORMATION SECURITY PROGRAM MANAGEMENT 5305.1

(Revised 8/2015)

Policy: Each state entity must provide for the proper use and protection of its information assets. Accordingly each state entity shall:

1. Develop, implement, and maintain a state entity-wide Information Security Program Plan.
2. Ensure the plan documentation provides the following:
    a. an overview of the requirements for the state entity's information security program;
    b. a description of the state entity's strategy and prioritization approach to information security, privacy, and risk management;
    c. a plan for integrating information security resource needs into the state entity's capital planning and funding request processes; and
    d. a plan of action and milestones (POAM) process for addressing program deficiencies. State entities shall use the standardized POAM reporting instructions and tool (SIMM 5305-B and SIMM 5305-C, respectively).
3. Ensure the plan is approved and disseminated by the state entity head responsible and accountable for risks incurred to the state entity's mission, functions, assets, image and reputation.
4. Identify roles and responsibilities, and assign management responsibilities for information security program management consistent with the roles and responsibilities described in the Information Security Program Management Standard (SIMM 5305-A).

Implementation Controls: NIST SP 800-53: Planning (PL); Program Management (PM); Information Security Program Management Standard (SIMM 5305-A); Plan of Action and Milestones (SIMM 5305-B and SIMM 5305-C)