

SAM – INFORMATION SECURITY
(Office of Information Security)

INFORMATION ASSET MANAGEMENT
(Revised 12/13)

5305.5

Introduction: In order to provide for the proper use and protection of information assets, the value and level of protection needed must be clearly specified and understood.

Policy: Each state entity must understand the value of its information assets and the level of protection those assets require. To this end, each state entity shall establish and maintain an inventory of all of its information assets, including information systems, information system components, and information repositories (both electronic and paper). The inventory shall contain a listing of all programs and information systems identified as collecting, using, maintaining, or sharing state entity information. The inventory must include categorization and classification of the information assets by program management, and based on the Information Security Program Management Standard ([SIMM 5305-A](#)), California Public Records Act ([Government Code sections 6250-6265](#)), Information Practices Act of 1977 ([Civil Code Section 1798, et seq.](#)), [FIPS Publication 199](#), and laws governing administration of the state entity's programs.

The categorization and classification of information assets shall be used in the determination of an asset's needed level of protection. If the information asset's level of protection is not clear, the state entity is to protect the asset to the categorization level of "Moderate" as defined by [FIPS Publication 199](#). Where the state entity is the custodian or user of the information asset, and not the owner, as in the case of Federal Tax Information, Criminal Justice Information Services information, and so forth the state entity shall ensure the data owner specifies the level of protection. The state entity shall adhere to the data owner's classification and level of protection requirements.

Each information asset for which the state entity has ownership responsibility shall be inventoried and identified to include the following:

1. Description and value of the information asset.
2. Owner of the information asset.
3. Custodians of the information asset.
4. Users of the information asset.
5. Classification of information.
6. [FIPS Publication 199](#) categorization and level of protection (Low, Moderate, or High).
7. Importance of information asset to the execution of the state entity's mission and program function.
8. Potential consequences and impacts if confidentiality, integrity and availability of the information asset were compromised.

Implementation Controls: NIST SP 800-53: [Planning \(PL\)](#); [Program Management \(PM\)](#); [Information Security Program Management Standard \(SIMM 5305-A\)](#); and [FIPS Publication 199](#).