ALABAMA DEPARTMENT OF FINANCE

Information Services Division

INFORMATION TECHNOLOGY STANDARD 500S2-00: SECURITY CATEGORIZATION OF STATE INFORMATION AND INFORMATION SYSTEMS

This standard establishes security categories for both information and information systems. These requirements are based on the methods described in FIPS Publication 199, "Standards for Security Categorization of Federal Information and Information Systems"; NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations"; and the US-DHS Cyber Security Evaluation Tool (CSET).

OBJECTIVE:

Promote effective management of information security programs by providing a common Security categorization framework and terminology for expressing the security assurance level (SAL) of State information and information systems.

SCOPE:

These requirements shall apply to all information and information systems hosted within the Information Services Division (ISD) address space.

REQUIREMENTS:

ISD shall use the security categorizations described herein in order to determine an appropriate set of security controls required to protect information and information systems.

SECURITY CATEGORIES OF INFORMATION AND INFORMATION SYSTEMS

Information, information systems, and applications are deployed in zones based on the level of security that is required to ensure the confidentiality, integrity, and availability of the data, the system, and of other systems deployed in the same zone.

There are (at least) five security zones that map to five defined security assurance levels: HIGH, MODERATE, LOW, ZERO, and AT RISK (additional security designators or zones may be developed and used at agency discretion). ISD shall use the Security Assurance Level Determination Checklist (contained herein) to determine the appropriate SAL and zone assignment.

Applicable security controls are applied to each respective zone. The mapping of information system SAL to a security zone will ensure that systems have the appropriate set of security controls applied.

DEFINITIONS

INFORMATION SYSTEM: a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [44 U.S.C., SEC. 3502] An information system could therefore be the physical or logical component devices that comprise or support an application or a website (for example).

SAL HIGH: when the unauthorized disclosure of information, the unauthorized modification or destruction of information, or the disruption of access to or use of information or an information system could be expected to have a ***severe or catastrophic*** adverse effect on organizational operations, organizational assets, or individuals that may, for example, (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries. SAL HIGH systems require the most restrictive set of security controls which may be costly and may also limit some desired functionality. Organizations need to make thoroughly researched risk-based decisions before designating a system as SAL HIGH.

SAL MODERATE: when the unauthorized disclosure of information, the unauthorized modification or destruction of information, or the disruption of access to or use of information or an information system could be expected to have a ***serious*** adverse effect on organizational operations, organizational assets, or individuals that may, for example, (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

SAL LOW: when the unauthorized disclosure of information, the unauthorized modification or destruction of information, or the disruption of access to or use of information or an information system could be expected to have a ***limited*** adverse effect on organizational operations, organizational assets, or individuals that may, for example (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals which may include, but is not limited to, loss of the privacy to which individuals are entitled under law.

SAL ZERO: when the unauthorized disclosure of information, the unauthorized modification or destruction of information, or the disruption of access to or use of information or an information system could be expected to have a ***very limited or no*** adverse effect on organizational operations, organizational assets, or individuals that may, for example (i) little or no degradation in mission capability or effectiveness; (ii) result in little or no damage to organizational assets; (iii) result in very minor or no financial loss; or (iv) result in no harm to individuals greater than the potential for inconvenience caused by, for example, missing or misrepresented information. For example, SAL ZERO systems may not store, communicate, or process any Privacy Act information.

SAL AT RISK: regardless of the information type or other factors that determine a system’s SAL, the information system will be considered AT RISK when it is not being actively managed and maintained (e.g., security patches applied), when it is operating on unsupported components, or when it is not compliant with specific policies and/or security controls required for its SAL/zone. Additional risk factors, including risk factors that are not known at the time the system was initially assessed, may also place an information system AT RISK. AT RISK systems require the application of additional security measures and a Plan of Action and Milestones (POA&M) for mitigating the risks. Once the risks are successfully mitigated, the system may revert to its previous SAL or to the appropriate SAL determined at that time.

SECURITY CONTROLS APPLICABLE TO EACH SAL/ZONE

HIGH: will utilize the current NIST 800-53 security control baseline for HIGH systems.

MODERATE: will utilize the current NIST 800-53 security control baseline for MODERATE systems.

LOW: will utilize the current NIST 800-53 security control baseline for LOW systems.

ZERO: applicable security controls will be determined based on a risk assessment.

AT RISK: applicable security controls will be determined based on a detailed risk assessment.

SECURITY ASSURANCE LEVEL DETERMINATION CHECKLIST

To determine the security assurance level (SAL) for an information system or application, evaluate it using the following checks.

Check #1: Is the information system primarily and routinely used to store, communicate, or process any of the following types of information?

- Emergency Response
- Key Asset & Critical Infrastructure Protection

If YES, then SAL is HIGH; continue with Check #5.

If NO, continue with Check #2.

Check #2: Is the information system primarily and routinely used to store, communicate, or process any of the following types of information?

- Collections & Receivables
- Contingency Planning
- Continuity of Operations
- Cost Accounting/Performance Measurement
- Energy Resource Management
- Energy Supply
- Environmental Remediation
- Information Management
- Information Security
- Lifecycle/Change Management
- Payments
- Percentage Infrastructure Maintenance
- Reporting Information
- Research & Development
- Scientific & Technical Research & Innovation
- Security Management
- System & Network Monitoring
- System Development
- System Maintenance

If YES, then SAL is MODERATE; continue with Check #5.

If NO, then SAL is LOW. Continue with Check #3.

Check #3: Is the system or application primarily used for sharing information intended for general public use (such as an informational website)?

If YES, then SAL is ZERO; continue with Check #5.

If NO, then SAL is LOW. Continue with Check #4.

Check #4: Questions about system impact (answer YES or NO)

4.1 Does aggregation of information on this system reveal sensitive patterns and plans, or facilitate access to sensitive or critical systems?

4.2 Would unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) adversely affect operations or seriously damage mission function and/or public confidence?

4.3 Would either physical or logical destruction of the system result in very large expenditures to restore the system and/or require a long period of time for recovery?

4.4 Does the mission served by the system, or the information that the system processes, affect the security of critical infrastructures and key resources?

4.5 Does the system store, communicate, or process any privacy act information?

4.6 Does the system store, communicate, or process any trade secrets information?

4.7 Are there any other extenuating circumstances that may require the SAL to be elevated to the next higher level (such as but not limited to: system provides critical process flow or security capability, public visibility of the system, the sheer number of other systems reliant on its operation, or the overall cost of system replacement)?

If the response to any of these questions was YES, then the SAL is MODERATE.

Continue with Check #5.

Check #5: Questions about system lifecycle management (answer YES or NO)

5.1 Are all of the information system's components (including but not limited to operating system, database system, development platform/framework, web server, and physical components) covered by vendor-support and/or warranty?

5.2 Is the information system compliant with all applicable information security policies?

5.3 Does information system maintenance follow a defined system lifecycle management plan?

If the response to any of these questions was NO, then the SAL is AT RISK.

ADDITIONAL INFORMATION:

Information Technology Policy 500: Statewide Information Systems Architecture
http://cybersecurity.alabama.gov/documents/Policy_500_Statewide_Info_Systems_Architecture.pdf

Information Technology Dictionary
http://cybersecurity.alabama.gov/documents/IT_Dictionary.pdf

By Authority of Director, Information Services Division, Department of Finance

DOCUMENT HISTORY:

Version	Release Date	Comments
500S2-00	10/14/2014	Defines information system categorization (Security Assurance Level - SAL) and SAL determination process