# Guideline for Mapping Types of Information and Information Systems to Security Categorization Levels

SP 800-60

# FISMA Legislation Overview (Public Law 107-347)

- Framework for ensuring effectiveness of Federal information security controls
- Government-wide management and oversight of risks including coordination of information security efforts
- Development and maintenance of minimum controls
- Mechanism for improved oversight of Federal agency information security programs.
- Acknowledges that commercially developed products offer effective information security solutions
- Recognizes that selection of specific security solutions should be left to individual agencies

# NIST FISMA Tasks

In accordance with the provisions of FISMA, the National Institute of Standards and Technology has been tasked to develop:

- Standards to be used by Federal agencies to categorize information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels
- Guideline for identification of national security information and information systems
- Guidelines recommending the types of information and information systems to be included in each category
- Minimum information security requirements (management, operational, and technical security controls) for information and information systems in each such category

# Categorization Standards

- Develop standards to be used by Federal agencies to categorize information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels –

- NIST Response:
  - –Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*.

  - –Final Publication NLT December 2003

# Identification of National Security Information and Information Systems

- Develop in conjunction with the Department of Defense, including the National Security Agency, guidelines for identifying an information system as a national security system

- NIST Response:

  – NIST Special Publication 800-59, "Guideline for Identifying an Information System as a National Security System"

# Mapping Guidelines

- Develop guidelines recommending the types of information and information systems to be included in each category described in FIPS 199 –

- NIST Response:
  - Special Publication 800-60, "Guide for Mapping Types of Federal Information and Information Systems to Security Categorization Levels"

  - Final Publication NLT June 2004

# Taxonomy Workshop

**Some general findings and comments:**

- **Data/information sensitivity is dependent on context.**
- **Data sensitivity and information system sensitivity must be analyzed independently.**
- **The context of data/information can be segmented into administrative activities common to all agencies and the mission-specific activities of a given agency.**
- **We need a standard process for determining the sensitivity of information we collect and maintain as that information relates to an agency's mission. FIPS 200 should provide a baseline process which includes sensitivity analysis, classification, and subsequent handling procedures.**
  - **A description of information categories for administrative activities common to all agencies**
  - **A standard process for agencies to develop information categories that are specific to their mission**
- **The confidentiality component of the FIPS 199 draft needs to address privacy.**

# Minimum Security Requirements

•Develop minimum information security requirements (i.e., management, operational, and technical security controls) for information and information systems in each such category –

•NIST Response:Federal Information Processing Standards (FIPS) Publication 200, "Minimum Security Controls for Federal Information and Information Systems"*

– Final Publication NLT December 2005

* Special Publication 800-53, "Minimum Security Controls for Federal Information and Information Systems," projected for final publication in April 2004, will provide interim guidance until completion and adoption of FIPS 200.

# Draft SP 800-60 Organization

1. Overview of FIPS 199 security objectives and categorization levels
2. Overview of the process for assignment of impact levels to information by type and general considerations relating to impact assignment
3. Guidelines for assigning mission information impact levels
4. Impact levels by type for administrative, management, and service information
5. Guidelines for system categorization

- Appendices:
  - Glossary
  - References
  - Sample mission information impact assignments
  - Legally mandated sensitivity/criticality properties

# Security Objectives and Categorization Levels

# FIPS 199

## Standards for Security Categorization of Federal Information and Information Systems

Applicability

- Applies to all unclassified information within the Federal government and all Federal information systems other than those information systems designated as national security systems
- Agency officials to use the security categorizations described in FIPS 199 whenever there is a Federal requirement to provide such a categorization of information or information systems
- Additional security designators may be developed and used at agency discretion.

# FIPS 199
## Impact Assessment

- **Context:**

  Agency security objectives and impacts resulting from compromise of information and information systems

- **Determination:**

  - Assumption that intentional or unintentional exploitation of particular vulnerabilities would result in loss of confidentiality, integrity, or availability
  - Potential impact/magnitude of harm resulting from loss would have on agency operations, assets, or individuals

# FIPS 199
## Security Objectives

- **Confidentiality:**

  A loss of *confidentiality* is the unauthorized disclosure of information.

- **Integrity:**

  A loss of *integrity* is the unauthorized modification or destruction of information.

- **Availability:**

  A loss of *availability* is the disruption of access to or use of information or an information system.

# FIPS 199
## Levels of Risk

- **Low**

  The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.

- **Moderate**

  – The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.

- **High**

  – The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

# FIPS 199
## Categorization

• The generalized format for expressing the security category, SC, of an information system is:

• $\mathbf{SC}_{\text{information system}} = \{(\textbf{confidentiality}, \textit{impact}), (\textbf{integrity}, \textit{impact}), (\textbf{availability}, \textit{impact})\}$,

where the acceptable values for potential impact are low, moderate, or high.

• The level of risk for confidentiality for *information systems* will never be zero.

# Definition of National Security Information and Information Systems

Any information system used or operated by an agency or on behalf of an agency –

- The function, operation, or use of which –
  - Involves intelligence activities
  -involves cryptologic activities related to national security
  - involves command and control of military forces
  - involves equipment that is an integral part of a weapon or weapons system
  - is critical to the direct fulfillment of military or intelligence missions*
- Is classified in the interests of national defense or foreign policy

* Does not include systems used for routine administrative or business applications.

# Process for Assignment of Impact Levels to Information By Type

- **Identify all of the information types that are input into, stored in, processed by, and/or output from each system under review.**
- **Provisionally assign default impact levels to each information type processed in and/or by each system under review.**
- **Review the appropriateness of the default impact levels in the context of the organization, environment, mission, use, and connectivity associated with the system under review.**
- **Adjustments should be made to the recommended default impact levels as appropriate.**
- **Employ system assessment guidelines provided in Sections 3 and 6 to establish the level of confidentiality impact, integrity impact, and availability impact associated with each system under review.**
- **Select the set of SP 800-53 security controls necessary for each system.**

# Guidelines for Identifying Mission Information Types

- CIO responsible for each system, or designee, is responsible for identifying the information types stored in, processed by, or generated by that system.
- For mission information, designated individual, in coordination with management, operational, and security stake holders, compiles:
  - Comprehensive set of lines of business conducted by the agency.
  - Functions and sub-functions necessary to conduct agency business within each line.
- Each sub-function within a line of business or mission area corresponds to an information type

# Guidelines for Assignment of Impact Levels to Mission Information

+ **Direct service missions provide the primary frame of reference for determining the impact levels and security objectives for government information and information systems.**

+ **The consequences of unauthorized disclosure of information, breach of information or information system integrity, and denial of information or information system services are defined by the nature and beneficiary(ies) of the service being provided or supported.**

+ **Using the categorization criteria identified in FIPS 199, assign impact levels and consequent security category for each mission information type identified for each system.**

# Impact Levels by Type for Administrative, Management, and Service Information

- OMB's Federal Enterprise Architecture Program Management Office's *Business Reference Model 1.0* is basis for defining information types.
- Agencies may identify additional information types.
- Using the categorization criteria identified in FIPS 199, assign impact levels and consequent security category for each information type.
- Default recommendations and discussion regarding rationale and deviations are suggested in the guideline.

# Administrative, Management, and Service Information

| Admin & Management Information | | |
|---|---|---|
| *Business Management of Information* | *Information Technology Management* | *Federal Financial Assistance* |
| Information Collection | IT Lifecycle/Change Management | Grants Assistance |
| Records Retention | IT System Development | Loan Assistance |
| Information Sharing | IT System Maintenance | Subsidies |
| *Controls and Oversight* | *Internal Risk Management/Mitigation* | *Legislative Management* |
| Corrective Action (Policy/Regulation) | Contingency Planning | Legislation Tracking |
| Program Evaluation | Continuity of Operations | Legislation Testimony |
| Program Monitoring | Service Recovery | Legislative Proposal Development |
| *Public Affairs* | *Regulatory Management* | *Planning & Resource Allocation* |
| Customer Services | Regulatory Policy & Guidance Development | Budget Formulation |
| Communications & Outreach | Public Comment Tracking | Capital Planning |
| Product Marketing | Regulatory Creation | Enterprise Architecture |
| Public Relations | Rule Publication | Project Planning |
| | | Strategic Planning |
| | | Budget Execution |
| **Service Support Information** | | |
| *Administration* | *Financial Management (Cont'd)* | *Human Resources* |
| Facilities/Fleet/Equipment Management | Funds Management | Personnel Advancement/Rewards |
| Help Desk Services | General Ledger Management | Personnel Benefits Management |
| IT Infrastructure Maintenance | Payment Management | Labor Management (Fed Employee) |
| Security Management | Receivables Management | Payroll Mgt/Expense Reimbursement |
| Administration of Travel | *Supply Chain Management* | Resource Training & Development |
| Intra-Agency Workplace Policy Dev & Mgt | Goods Acquisition | Security Clearance Management |
| *Financial Management* | Inventory Control | Staff Recruitment & Employment |
| Cost Management | Logistics Management | |
| Financial Reporting | Services Acquisition | |

# Guidelines for System Categorization

Information system requires more complex analysis than information types and must consider both:

(i) the security categories of all information types resident on the information system; and

(ii) the security category of the hardware and software (including application and system-level programs) that comprise the information system and are necessary for an agency to conduct its essential mission-related operations.

Primary factors that most commonly raise the total system impact:

+ Aggregation
+ Connectivity
+ Critical system functionality.

# Draft SP 800-60

- Overview of FIPS 199 security objectives and categorization levels
- Overview of the process for assignment of impact levels to information by type and general considerations relating to impact assignment
- Guidelines for assigning mission information impact levels
- Impact levels by type for administrative, management, and service information
- Guidelines for system categorization
- Appendices:
  - Sample mission information impact assignments
  - Legally mandated sensitivity/criticality properties