FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of Federal Information and Information Systems

---

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

February 2004

U.S. DEPARTMENT OF COMMERCE
Donald L. Evans, Secretary

TECHNOLOGY ADMINISTRATION
Phillip J. Bond, Under Secretary for Technology

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Arden L. Bement, Jr., Director

FOREWORD

The Federal Information Processing Standards Publication Series of the National Institute of Standards and Technology (NIST) is the official series of publications relating to standards and guidelines adopted and promulgated under the provisions of Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Federal Information Security Management Act of 2002 (Public Law 107-347). These mandates have given the Secretary of Commerce and NIST important responsibilities for improving the utilization and management of computer and related telecommunications systems in the federal government. The NIST, through its Information Technology Laboratory, provides leadership, technical guidance, and coordination of government efforts in the development of standards and guidelines in these areas.

Comments concerning Federal Information Processing Standards Publications are welcomed and should be addressed to the Director, Information Technology Laboratory, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900.

-- SUSAN ZEVIN, ACTING DIRECTOR
INFORMATION TECHNOLOGY LABORATORY

AUTHORITY

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Federal Information Security Management Act of 2002 (Public Law 107-347).

TABLE OF CONTENTS

1 PURPOSE

The E-Government Act of 2002 (Public Law 107-347), passed by the one hundred and seventh Congress and signed into law by the President in December 2002, recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act of 2002 (FISMA), tasked NIST with responsibilities for standards and guidelines, including the development of:

- Standards to be used by all federal agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels;
- Guidelines recommending the types of information and information systems to be included in each category; and
- Minimum information security requirements (i.e., management, operational, and technical controls), for information and information systems in each such category.

FIPS Publication 199 addresses the first task cited—to develop standards for categorizing information and information systems. Security categorization standards for information and information systems provide a common framework and understanding for expressing security that, for the federal government, promotes: (i) effective management and oversight of information security programs, including the coordination of information security efforts throughout the civilian, national security, emergency preparedness, homeland security, and law enforcement communities; and (ii) consistent reporting to the Office of Management and Budget (OMB) and Congress on the adequacy and effectiveness of information security policies, procedures, and practices. Subsequent NIST standards and guidelines will address the second and third tasks cited.

2 APPLICABILITY

These standards shall apply to: (i) all information within the federal government other than that information that has been determined pursuant to Executive Order 12958, as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status; and (ii) all federal information systems other than those information systems designated as national security systems as defined in 44 United States Code Section 3542(b)(2). Agency officials shall use the security categorizations described in FIPS Publication 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. State, local, and tribal governments as well as private sector organizations comprising the critical infrastructure of the United States may consider the use of these standards as appropriate. These standards are effective upon approval by the Secretary of Commerce.

3 CATEGORIZATION OF INFORMATION AND INFORMATION SYSTEMS

This publication establishes security categories for both information[1] and information systems. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.

[1] Information is categorized according to its *information type*. An information type is a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, Executive Order, directive, policy, or regulation.

Security Objectives

The FISMA defines three security objectives for information and information systems:

CONFIDENTIALITY

"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542]

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

INTEGRITY

"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542]

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

AVAILABILITY

"Ensuring timely and reliable access to and use of information…" [44 U.S.C., SEC. 3542]

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

Potential Impact on Organizations and Individuals

FIPS Publication 199 defines three levels of *potential impact* on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). The application of these definitions must take place within the context of each organization and the overall national interest.

The *potential impact* is **LOW** if—

– The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.[2]

A

The *potential impact* is **HIGH** if—

– 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.

AMPLIFICATION: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (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.

Security Categorization Applied to Information Types

The security category of an information type can be associated with both user information and system information[3] and can be applicable to information in either electronic or non-electronic form. It can also be used as input in considering the appropriate security category of an information system (see description of security categories for information systems below). Establishing an appropriate security category of an information type essentially requires determining the *potential impact* for each security objective associated with the particular information type.

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

SC information type = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)},

where the acceptable values for potential impact are LOW, MODERATE, HIGH, or NOT APPLICABLE.[4]

EXAMPLE 1: An organization managing *public information* on its web server determines that there is no potential impact from a loss of confidentiality (i.e., confidentiality requirements are not applicable), a moderate potential impact from a loss of integrity, and a moderate potential impact from a loss of availability. The resulting security category, SC, of this information type is expressed as:

SC public information = {(**confidentiality**, NA), (**integrity**, MODERATE), (**availability**, MODERATE)}.

EXAMPLE 2: A law enforcement organization managing extremely sensitive *investigative information* determines that the potential impact from a loss of confidentiality is high, the potential impact from a loss of integrity is moderate, and the potential impact from a loss of availability is moderate. The resulting security category, SC, of this information type is expressed as:

SC investigative information = {(**confidentiality**, HIGH), (**integrity**, MODERATE), (**availability**, MODERATE)}.

EXAMPLE 3: A financial organization managing routine *administrative information* (not privacy-related information) determines that the potential impact from a loss of confidentiality is low, the potential impact from a loss of integrity is low, and the potential impact from a loss of availability is low. The resulting security category, SC, of this information type is expressed as:

SC administrative information = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}.

[3] System information (e.g., network routing tables, password files, and cryptographic key management information) must be protected at a level commensurate with the most critical or sensitive user information being processed, stored, or transmitted by the information system to ensure confidentiality, integrity, and availability.

[4] The potential impact value of *not applicable* only applies to the security objective of confidentiality.

Security Categorization Applied to Information Systems

Determining the security category of an information system requires slightly more analysis and must consider the security categories of all information types resident on the information system. For an information system, the potential impact values assigned to the respective security objectives (confidentiality, integrity, availability) shall be the highest values (i.e., high water mark) from among those security categories that have been determined for each type of information resident on the information system.[5]

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

SC information system = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)},

where the acceptable values for potential impact are LOW, MODERATE, or HIGH.

Note that the value of *not applicable* cannot be assigned to any security objective in the context of establishing a security category for an information system. This is in recognition that there is a low minimum potential impact (i.e., low water mark) on the loss of confidentiality, integrity, and availability for an information system due to the fundamental requirement to protect the system-level processing functions and information critical to the operation of the information system.

EXAMPLE 4: An information system used for large acquisitions in a contracting organization contains both sensitive, pre-solicitation phase contract information and routine administrative information. The management within the contracting organization determines that: (i) for the sensitive contract information, the potential impact from a loss of confidentiality is moderate, the potential impact from a loss of integrity is moderate, and the potential impact from a loss of availability is low; and (ii) for the routine administrative information (non-privacy-related information), the potential impact from a loss of confidentiality is low, the potential impact from a loss of integrity is low, and the potential impact from a loss of availability is low. The resulting security categories, SC, of these information types are expressed as:

SC contract information = {(**confidentiality**, MODERATE), (**integrity**, MODERATE), (**availability**, LOW)},

and

SC administrative information = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}.

The resulting security category of the information system is expressed as:

SC acquisition system = {(**confidentiality**, MODERATE), (**integrity**, MODERATE), (**availability**, LOW)},

representing the high water mark or maximum potential impact values for each security objective from the information types resident on the acquisition system.

[5] It is recognized that information systems are composed of both programs and information. Programs in execution within an information system (i.e., system processes) facilitate the processing, storage, and transmission of information and are necessary for the organization to conduct its essential mission-related functions and operations. These system processing functions also require protection and could be subject to security categorization as well. However, in the interest of simplification, it is assumed that the security categorization of all information types associated with the information system provide an appropriate *worst case* potential impact for the overall information system—thereby obviating the need to consider the system processes in the security categorization of the information system.

EXAMPLE 5: A power plant contains a SCADA (supervisory control and data acquisition) system controlling the distribution of electric power for a large military installation. The SCADA system contains both real-time sensor data and routine administrative information. The management at the power plant determines that: (i) for the sensor data being acquired by the SCADA system, there is no potential impact from a loss of confidentiality, a high potential impact from a loss of integrity, and a high potential impact from a loss of availability; and (ii) for the administrative information being processed by the system, there is a low potential impact from a loss of confidentiality, a low potential impact from a loss of integrity, and a low potential impact from a loss of availability. The resulting security categories, SC, of these information types are expressed as:

SC sensor data = {(**confidentiality**, NA), (**integrity**, HIGH), (**availability**, HIGH)},

and

SC administrative information = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}.

The resulting security category of the information system is initially expressed as:

SC SCADA system = {(**confidentiality**, LOW), (**integrity**, HIGH), (**availability**, HIGH)},

representing the high water mark or maximum potential impact values for each security objective from the information types resident on the SCADA system. The management at the power plant chooses to increase the potential impact from a loss of confidentiality from low to moderate reflecting a more realistic view of the potential impact on the information system should there be a security breach due to the unauthorized disclosure of system-level information or processing functions. The final security category of the information system is expressed as:

SC SCADA system = {(**confidentiality**, MODERATE), (**integrity**, HIGH), (**availability**, HIGH)}.

Table 1 summarizes the potential impact definitions for each security objective—confidentiality, integrity, and availability.

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	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.	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.	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.

TABLE 1: POTENTIAL IMPACT DEFINITIONS FOR SECURITY OBJECTIVES

APPENDIX A TERMS AND DEFINITIONS

AVAILABILITY: Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]

CONFIDENTIALITY: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]

EXECUTIVE AGENCY: An executive department specified in 5 U.S.C., SEC. 101; a military department specified in 5 U.S.C., SEC. 102; an independent establishment as defined in 5 U.S.C., SEC. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., CHAPTER 91. [41 U.S.C., SEC. 403]

FEDERAL INFORMATION SYSTEM: An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency. [40 U.S.C., SEC. 11331]

INFORMATION: An instance of an information type.

INFORMATION RESOURCES: Information and related resources, such as personnel, equipment, funds, and information technology. [44 U.S.C., SEC. 3502]

INFORMATION SECURITY: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. [44 U.S.C., SEC. 3542]

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]

INFORMATION TECHNOLOGY: Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. [40 U.S.C., SEC. 1401]

INFORMATION TYPE: A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management), defined by an organization, or in some instances, by a specific law, Executive Order, directive, policy, or regulation.

INTEGRITY: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]

NATIONAL SECURITY SYSTEM: Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency— (i) 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; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or, (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. [44 U.S.C., SEC. 3542]

SECURITY CATEGORY: The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.

SECURITY CONTROLS: The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

SECURITY OBJECTIVE: Confidentiality, integrity, or availability.

APPENDIX B REFERENCES

[1] Privacy Act of 1974 (Public Law 93-579), September 1975.

[2] Paperwork Reduction Act of 1995 (Public Law 104-13), May 1995.

[3] OMB Circular A-130, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.

[4] Information Technology Management Reform Act of 1996 (Public Law 104-106), August 1996.

[5] Federal Information Security Management Act of 2002 (Public Law 107-347), December 2002.