FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of Federal Information and Information Systems

INITIAL PUBLIC DRAFT

VERSION 1.0

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

May 2003

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 0f 2002 (Public Law 107-347).

TABLE OF CONTENTS

1 INTRODUCTION

The E-Government Act (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 (FISMA), requires each Federal agency to develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. The information security program must include—

- Periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency;
- Policies and procedures that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level, and ensure that information security is addressed throughout the life cycle of each agency information system;
- Subordinate plans for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate;
- Security awareness training to inform personnel (including contractors and other users of information systems that support the operations and assets of the agency) of the information security risks associated with their activities and their responsibilities in complying with agency policies and procedures designed to reduce these risks;
- Periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices (including the management, operational, and technical controls of every agency information system identified in their inventory) to be performed with a frequency depending on risk, but no less than annually;
- A process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures and practices of the agency;
- Procedures for detecting, reporting, and responding to security incidents (including mitigating risks associated with such incidents before substantial damage is done and notifying and consulting with the Federal information security incident response center, and as appropriate, law enforcement agencies, relevant Offices of Inspector General, and any other agency or office, in accordance with law or as directed by the President; and
- Plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

In accordance with the provisions of FISMA, heads of Federal agencies are responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification or destruction of: (i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. Agency heads are also responsible for ensuring that information security management processes are integrated with agency strategic and operational planning processes. In addition to the above responsibilities, agency heads must ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control including through—

- Assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;

- Determining the levels of information security appropriate to protect such information and information systems in accordance with standards promulgated by the National Institute of Standards and Technology (NIST), for information security categorization and related requirements;
- Implementing policies and procedures to cost-effectively reduce risks to an acceptable level; and
- Periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented.

FISMA, along with the Paperwork Reduction Act of 1995 and the Information Technology Management Reform Act of 1996 (Clinger-Cohen Act), explicitly emphasizes a risk-based policy for cost-effective security.

2 PURPOSE

FISMA tasked NIST 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;
- 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 security controls), for information and information systems in each such category.

The NIST response to these three tasks will provide Federal agencies with a standard means of determining the baseline security controls for the information and information systems identified in the agency's inventory in accordance with 44 United States Code Section 3505(c). The standards described in the first task will define requirements for categorizing information and information systems according to a range of risk levels for the security objectives of confidentiality, integrity, and availability. The guidelines resulting from the second task will help agencies identify, in a consistent manner, the types of information, (e.g., privacy information, mission critical information, operational information, medical information, proprietary information, financial information, contractor sensitive information, trade secret information, investigation information, new technology and controlled scientific information, system configuration and management information) and information systems appropriate for each category. Finally, the standards resulting from the third task will describe minimum sets of security controls for information and information systems for each defined category. FIPS Publication 199 addresses the first of these three tasks.

Security categorization standards for Federal information and information systems provide a common framework and understanding that promotes: (i) effective government-wide management and oversight of Federal agency information security programs, including the coordination of information security efforts throughout the civilian, national security, and law enforcement communities, and (ii) consistent agency reporting to the Office of Management and Budget (OMB) and Congress on the adequacy and effectiveness of information security policies, procedures, and practices.

3 APPLICABILITY

This standard shall apply to: (i) all information within the Federal government other than that information that has been determined pursuant to Executive Order 12958 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 this standard 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.

4 TERMS AND DEFINITIONS

The terms and definitions in this section are applicable to this FIPS publication and have been obtained from Congressional legislation, Executive Orders, OMB policies, and commonly accepted glossaries of security terminology.

AUTHENTICATION: Security control designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

AUTHENTICITY: The property of being genuine and able to be verified and be trusted. See authentication.

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]

COUNTERMEASURES: Synonymous with security controls and safeguards.

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 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: (1) requires the use of such equipment, or (2) 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]

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]

NON-REPUDIATION: Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later legitimately deny having processed, stored, or transmitted the information.

RESIDUAL RISK: The portion of risk remaining after appropriate security controls have been applied.

RISK: A combination of: (i) the likelihood that a particular vulnerability in an agency information system will be either intentionally or unintentionally exploited by a particular threat resulting in a loss of confidentiality, integrity, or availability, and (ii) the potential impact or magnitude of harm that a loss of confidentiality, integrity, or availability will have on an agency's operations (including mission, functions, image or reputation), an agency's assets, or individuals (including privacy) should the exploitation occur.

RISK ASSESSMENT: A key component of risk management that brings together important information for agency officials with regard to the protection of information and information systems including the identification of: (i) threats and vulnerabilities, and (ii) the potential impact or magnitude of harm that a loss of confidentiality, integrity, or availability would have on agency operations (including mission, functions, image or reputation), agency assets, or individuals (including privacy) should there be a threat exploitation of information system vulnerabilities.

RISK MANAGEMENT: The process of identifying, controlling, and mitigating risks. It includes: risk assessment, cost benefit analysis, and the selection, implementation, testing and evaluation of security controls.

SAFEGUARDS: Synonymous with security controls and countermeasures.

SECURITY CONTROLS: The management, operational, and technical controls (safeguards or countermeasures) prescribed for an information system which, taken together, satisfy the specified security requirements and adequately protect the confidentiality, integrity, and availability of the system and its information.

THREAT: Any circumstance or event with the potential to intentionally or unintentionally exploit a specific vulnerability in an information system resulting in a loss of confidentiality, integrity, or availability.

VULNERABILITY: A flaw or weakness in the design or implementation of an information system (including the security procedures and security controls associated with the system) that could be intentionally or unintentionally exploited to adversely effect an agency's operations (including mission, functions, image or reputation), an agency's assets, or individuals (including privacy) through a loss of confidentiality, integrity, or availability.

5 SECURITY CONTROLS AND RISK

There are three important questions that must be answered by agency officials when addressing the security considerations for their information and information systems:

- **SELECTION OF SECURITY CONTROLS:** What security controls are needed to adequately protect the information and information systems that support the operations and assets of the agency in order to accomplish its assigned missions, preserve its image or reputation, protect its assets, maintain its day-to-day functions, and protect individuals (including privacy)?
- **IMPLEMENTATION OF SECURITY CONTROLS:** Have the selected security controls been implemented or is there a realistic plan for their implementation?
- **ASSURANCE OF SECURITY CONTROLS:** What is the desired level of assurance, (i.e., grounds for confidence), that the selected security controls, as implemented, are effective in their application?

The answers to these questions cannot be given in isolation. They must be given in the context of an information security program for the agency that identifies, controls, and mitigates risks to its information and information systems. Risk is determined by assessing: (i) the likelihood that particular vulnerabilities in an agency information system would be either intentionally or unintentionally exploited by particular threats resulting in a loss of confidentiality, integrity, or availability, and (ii) the potential impact or magnitude of harm that the loss of confidentiality, integrity, or availability would have on agency operations (including mission, functions, image or reputation), agency assets, or individuals (including privacy) should the exploitation occur. Risk assessments, conducted in accordance with agency-selected methodologies, typically estimate the level of risk associated with information and information systems employed by the agency.

6 CATEGORIZATION OF INFORMATION AND INFORMATION SYSTEMS

This publication establishes three potential levels of risk (low, moderate, and high) for each of the stated security objectives (confidentiality, integrity, and availability) relevant to securing Federal information and information systems. The levels of risk consider both impact and threat, but are more heavily weighted toward impact. The impact is based on the potential magnitude of harm that the loss of confidentiality, integrity, or availability would have on agency operations (including mission, functions, image or reputation), agency assets, or individuals (including privacy). Threat information (including capability, intent, and resources of potential adversaries) for a specific information system or type of information is generally non-specific or incomplete at best. Recognizing the highly networked nature of the current Federal computing environment, this document acknowledges the existence of baseline threats to all information and information systems. In other words, in today's interconnected and interdependent information systems environment, which encompasses many common platforms and technologies, there is a high likelihood of a variety of threats (both malicious and unintentional) acting to compromise the security of information and information systems. Accordingly, the levels of risk focus on what is known about the potential *impact* or *harm* that could arise if certain events occur and the information and information system are not available to accomplish the agency's assigned mission, preserve its image or reputation, protect its assets, maintain its day-to-day functions and protect individuals (including privacy).

Levels of Risk

The level of risk is **low** if—

The event could be expected to have a limited adverse effect on agency operations (including mission, functions, image or reputation), agency assets, or individuals.[1] *The event could be expected to cause a negative outcome or result in limited damage to operations or assets, requiring minor corrective actions or repairs.*

[1] Adverse effects on individuals may include, but are not limited to, harm to the privacy to which individuals are entitled under law.

The level of risk is **moderate** if—

The event could be expected to have a serious adverse effect on agency operations (including mission, functions, image or reputation), agency assets, or individuals. The event could be expected to cause significant degradation in mission capability, place the agency at a significant disadvantage, or result in major damage to assets, requiring extensive corrective actions or repairs.

The level of risk is **high** if—

The event could be expected to have a severe or catastrophic adverse effect on agency operations (including mission, functions, image or reputation), agency assets, or individuals. The event could be expected to cause a loss of mission capability for a period that poses a threat to human life, or results in a loss of major assets.

Security Objectives and Types of Potential Losses

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.

Based on the assignment of appropriate levels of risk (low, moderate, or high) to the respective security objectives (confidentiality, integrity, and availability), information and information systems can be fully categorized with respect to security. The standardized format for documenting such security categories, (e.g., in security plans and risk assessments), is as follows:

CATEGORIZATION = [(**confidentiality**, RISK-LEVEL), (**integrity**, RISK-LEVEL), (**availability**, RISK-LEVEL)].

It is recognized that an information system may contain more than one type of information, (e.g., privacy information, medical information, proprietary information, financial information, contractor sensitive information), each of which is subject to security categorization. The security categorization of an *information system* that processes, stores, or transmits multiple types of information shall be at least the highest risk level that has been determined for each type of information for each security objective of confidentiality, integrity, and availability—taking into account dependencies among these objectives. For example, a substantial amount of *information* within Federal agencies requires no confidentiality protection and for such information, the level of risk for confidentiality is zero. However, the level of risk for confidentiality for *information systems* processing such information is not zero. In order to achieve information integrity and availability, some information must be protected against unauthorized disclosure; for example, passwords, cryptographic keys, and any other information that would facilitate a successful attack.

Table 1 summarizes the three levels of risk and associated descriptions for each security objective—confidentiality, integrity, and availability.

TABLE 1: CATEGORIZATION OF FEDERAL INFORMATION AND INFORMATION SYSTEMS

	LEVEL OF RISK		
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 agency operations (including mission, functions, image or reputation), agency assets, or individuals. A loss of confidentiality could be expected to cause a negative outcome or result in limited damage to operations or assets, requiring minor corrective actions or repairs.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on agency operations (including mission, functions, image or reputation), agency assets, or individuals. A loss of confidentiality could be expected to cause **significant degradation in mission capability, place the agency at a significant disadvantage**, or result in **major** damage to assets, requiring **extensive** corrective actions or repairs.	The unauthorized disclosure of information could be expected to have a **severe** or **catastrophic** adverse effect on agency operations (including mission, functions, image or reputation), agency assets, or individuals. A loss of confidentiality could be expected to cause **a loss of mission capability for a period that poses a threat to human life, or results in a loss of major assets**.
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 agency operations (including mission, functions, image or reputation), agency assets, or individuals. A loss of integrity could be expected to cause a negative outcome or result in limited damage to operations or assets, requiring minor corrective actions or repairs.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on agency operations (including mission, functions, image or reputation), agency assets, or individuals. A loss of integrity could be expected to cause **significant degradation in mission capability, place the agency at a significant disadvantage**, or result in **major** damage to assets, requiring **extensive** corrective actions or repairs.	The unauthorized modification or destruction of information could be expected to have a **severe** or **catastrophic** adverse effect on agency operations, (including mission, functions, image or reputation), agency assets, or individuals. A loss of integrity could be expected to cause **a loss of mission capability for a period that poses a threat to human life, or results in a loss of major assets**.
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 agency operations (including mission, functions, image or reputation), agency assets, or individuals. A loss of availability could be expected to cause a negative outcome or result in limited damage to operations or assets, requiring minor corrective actions or repairs.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on agency operations (including mission, functions, image or reputation), agency assets, or individuals. A loss of availability could be expected to cause **significant degradation in mission capability, place the agency at a significant disadvantage**, or result in **major** damage to assets, requiring **extensive** corrective actions or repairs.	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 agency operations (including mission, functions, image or reputation), agency assets, or individuals. A loss of availability could be expected to cause **a loss of mission capability for a period that poses a threat to human life, or results in a loss of major assets**.

7 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 No. A-130, Appendix III, "Security of Federal Automated Information Resources", February 1996.

[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.