Standards for the Security Categorization of Federal Information and Information Systems

Federal Information Processing Standards
FIPS Publication 199
Initial Public Draft

National Institute of Standards and Technology

Introduction

IAW the provisions of the Federal Information Security Management Act (FISMA), NIST 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
- 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

Purpose

Draft FIPS Publication 199 satisfies the first of the three FISMA requirements---

- To establish 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

Result

- Federal agencies will have a standard means of determining what baseline 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)

Applicability

The standard shall apply to:

- 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
- 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)

Security Objectives

- Confidentiality
  - ✓ "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542]
- Integrity
  - ✓ "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542]
- Availability
  - ✓ "Ensuring timely and reliable access to and use of information…" [44 U.S.C., Sec. 3542]

Types of Potential Losses

- Loss of Confidentiality
  - ✓ The unauthorized disclosure of information, including that in an information system---
- Loss of Integrity
  - ✓ The unauthorized modification or destruction of information, including that in an information system---
- Loss of Availability
  - ✓ The disruption of access to or use of information or an information system or the use of the processing capability of an information system for unauthorized purposes---

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. The event causes a negative outcome or results in limited damage to operations or assets, requiring minor corrective actions or repairs.*
- 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 causes significant degradation in mission capability, places the agency at a significant disadvantage, or results 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 causes a loss of mission capability for a period that poses a threat to human life, or results in a loss of major assets.*

Security Categorization

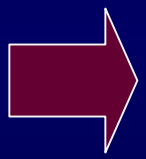
Risk Levels

Security Objective	Low	Moderate	High
Confidentiality	The unauthorized disclosure of information, including that in 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 confidentiality causes a negative outcome or results in limited damage to operations or assets, requiring minor corrective actions or repairs.	The unauthorized disclosure of information, including that in 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 confidentiality causes **significant degradation in mission capability, places the agency at a significant disadvantage**, or results in **major** damage to assets, requiring **extensive** corrective actions or repairs.	The unauthorized disclosure of information, including that in 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 confidentiality causes **a loss of mission capability for a period that poses a threat to human life, or results in a loss of major assets**.
Integrity	The unauthorized modification or destruction of information, including that in 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 integrity causes a negative outcome or results in limited damage to operations or assets, requiring minor corrective actions or repairs.	The unauthorized modification or destruction of information, including that in 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 integrity causes **significant degradation in mission capability, places the agency at a significant disadvantage**, or results in **major** damage to assets**,** requiring **extensive** corrective actions or repairs.	The unauthorized modification or destruction of information, including that in 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 integrity causes **a loss of mission capability for a period that poses a threat to human life, or results in a loss of major assets**.
Availability	The disruption of access to or use of information or an information system or the use of the processing capability of an information system for unauthorized purposes 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 causes a negative outcome or results 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 or the use of the processing capability of an information system for unauthorized purposes 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 causes **significant degradation in mission capability, places the agency at a significant disadvantage**, or results in **major** damage to assets, requiring **extensive** corrective actions or repairs.	The disruption of access to or use of information or an information system or the use of the processing capability of an information system for unauthorized purposes 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 causes **a loss of mission capability for a period that poses a threat to human life, or results in a loss of major assets**.

Security Categorization

An Example: Mission Critical Information and Information System

Guidance for Mapping Types of Federal Information and Information Systems to Draft FIPS Pub 199 Security Categories



Security Objective	Low	Moderate	High
Confidentiality	The unauthorized disclosure of information, including that in 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 confidentiality causes a negative outcome or results in limited damage to operations or assets, requiring minor corrective actions or repairs.	The unauthorized disclosure of information, including that in 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 confidentiality causes **significant degradation in mission capability, places the agency at a significant disadvantage**, or results in **major** damage to assets, requiring **extensive** corrective actions or repairs.	The unauthorized disclosure of information, including that in 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 confidentiality causes **a loss of mission capability for a period that poses a threat to human life, or results in a loss of major assets**.
Integrity	The unauthorized modification or destruction of information, including that in 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 integrity causes a negative outcome or results in limited damage to operations or assets, requiring minor corrective actions or repairs.	The unauthorized modification or destruction of information, including that in 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 integrity causes **significant degradation in mission capability, places the agency at a significant disadvantage**, or results in **major** damage to assets, requiring **extensive** corrective actions or repairs.	The unauthorized modification or destruction of information, including that in 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 integrity causes **a loss of mission capability for a period that poses a threat to human life, or results in a loss of major assets**.
Availability	The disruption of access to or use of information or an information system or the use of the processing capability of an information system for unauthorized purposes 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 causes a negative outcome or results 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 or the use of the processing capability of an information system for unauthorized purposes 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 causes **significant degradation in mission capability, places the agency at a significant disadvantage**, or results in **major** damage to assets, requiring **extensive** corrective actions or repairs.	The disruption of access to or use of information or an information system or the use of the processing capability of an information system for unauthorized purposes 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 causes **a loss of mission capability for a period that poses a threat to human life, or results in a loss of major assets**.

Security Categorization

Confidentiality = Moderate Integrity = High Availability = High

Guidance for Mapping Types of Federal Information and Information Systems to Draft FIPS Pub 199 Security Categories

Security Objective	Low	Moderate	High
Confidentiality	The unauthorized disclosure of information, including that in 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 confidentiality causes a negative outcome or results in limited damage to operations or assets, requiring minor corrective actions or repairs.	The unauthorized disclosure of information, including that in 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 confidentiality causes **significant degradation in mission capability, places the agency at a significant disadvantage**, or results in **major** damage to assets, requiring **extensive** corrective actions or repairs.	The unauthorized disclosure of information, including that in 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 confidentiality causes **a loss of mission capability for a period that poses a threat to human life, or results in a loss of major assets**.
Integrity	The unauthorized modification or destruction of information, including that in 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 integrity causes a negative outcome or results in limited damage to operations or assets, requiring minor corrective actions or repairs.	The unauthorized modification or destruction of information, including that in 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 integrity causes **significant degradation in mission capability, places the agency at a significant disadvantage**, or results in **major** damage to assets, requiring **extensive** corrective actions or repairs.	The unauthorized modification or destruction of information, including that in an information system, could be expected to have a **severe** or **catastroph** agency operations, (including mage or reputation), agency ass loss of integrity causes **a los lity for a period that poses a fe, or results in a loss of maj**
Availability	The disruption of access to or use of information or an information system or the use of the processing capability of an information system for unauthorized purposes 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 causes a negative outcome or results 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 or the use of the processing capability of an information system for unauthorized purposes 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 causes **significant degradation in mission capability, places the agency at a significant disadvantage**, or results in **major** damage to assets, requiring **extensive** corrective actions or repairs.	The disruption nformation or an information sy e processing capability of an in unauthorized purposes could be **vere** or **catastrophic** adverse erations (including mission, fun utation), agency assets, or individ bility causes **a loss of mission ca d that poses a threat to human loss of major assets**.

Minimum Security Controls for High Level of Risk for Integrity

Publication Schedule

- Federal Register announcement and initial public draft
  (March 2003)
- Public comment period #1
  (April-May 2003)
- Second public draft
  (August 2003)
- Public comment period #2
  (September-October 2003)
- Final publication
  (December 2003)

Contact Information

100 Bureau Drive Mailstop 8930
Gaithersburg, MD USA 20899-8930

Program Manager
Dr. Ron S. Ross
(301) 975-5390
rross@nist.gov

Assessment Scheme
Arnold Johnson
(301) 975-3247
arnold.johnson@nist.gov

Special Publications
Marianne Swanson
(301) 975-3293
marianne.swanson@nist.gov

Organization Accreditations
Patricia Toth
(301) 975-5140
patricia.toth@nist.gov

Gov't and Industry Outreach
Dr. Stu Katzke
(301) 975-4768
skatzke@nist.gov

Technical Advisor
Gary Stoneburner
(301) 975-5394
gary.stoneburner@nist.gov

Comments to: sec-cert@nist.gov
World Wide Web: http://csrc.nist.gov/sec-cert