Unit #3

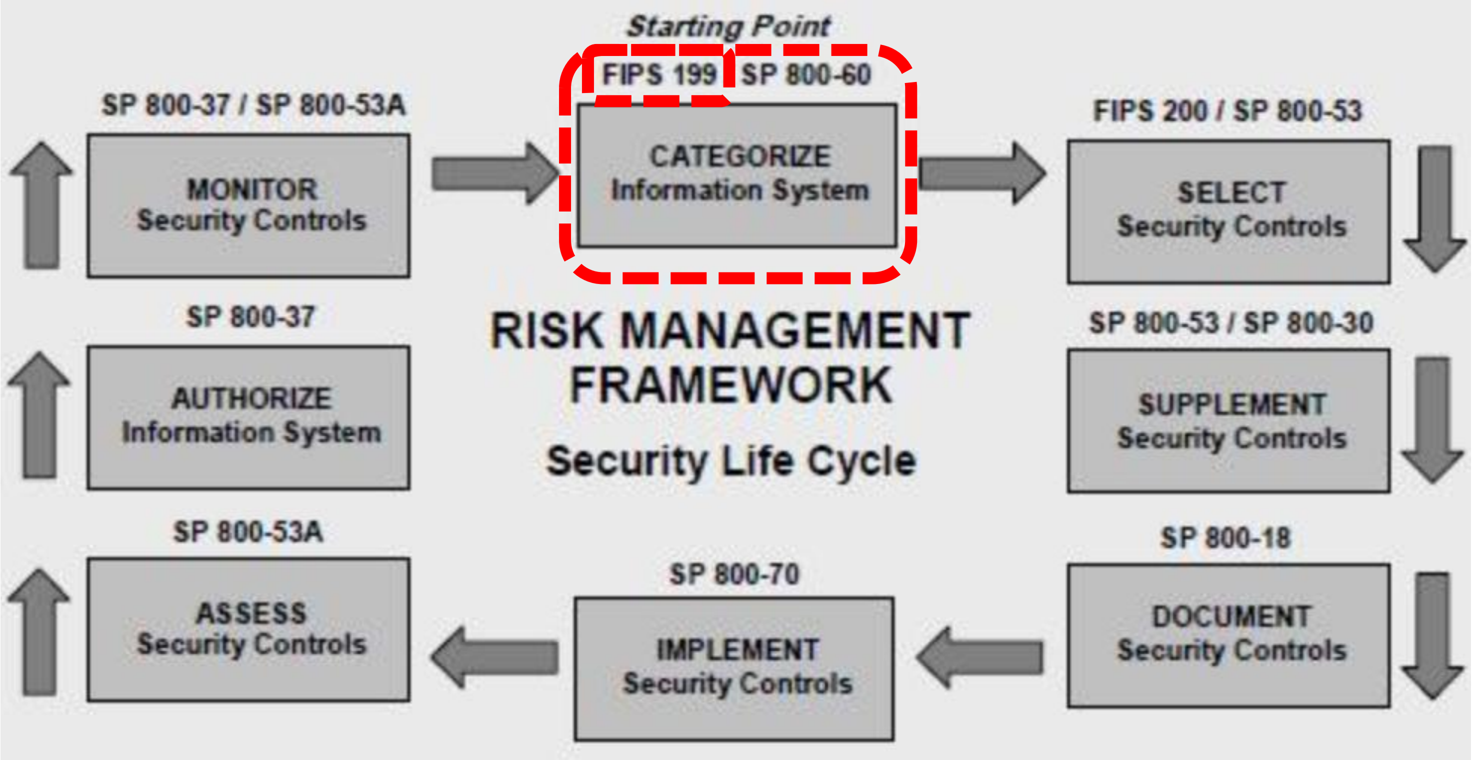
MIS5214

Planning and Policy

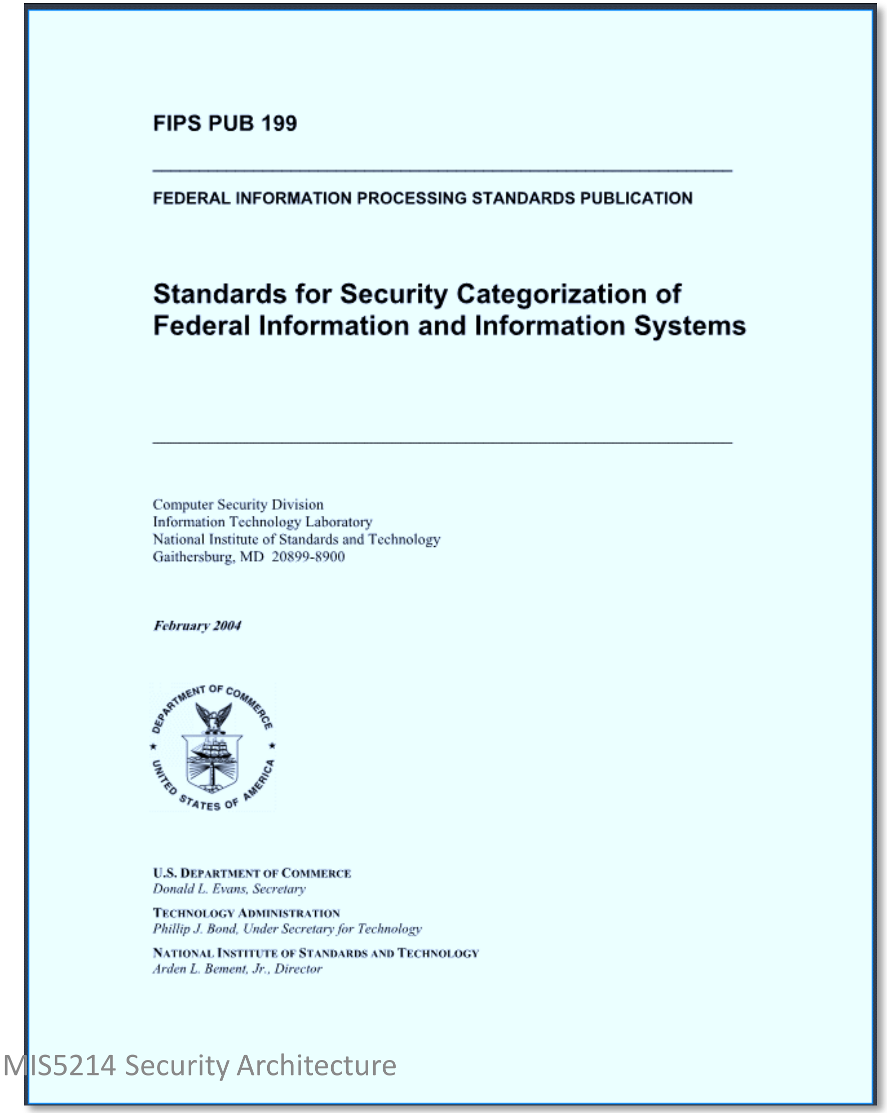
Agenda

- Risk Management Framework and IS Security Categorization
- Mapping Information Types to Security Categorizations
- Exercise: How to assess and information security policy?
- *Exercise – Determine Information and Information System Types and provisional security categorization*
- Security Control Baselines – review
    - Minimum Security Controls and Security Control Baselines
    - Security Control Families
- Risk Assessment Controls

Risk Management Framework



Risk Assessment based on security objectives and impact ratings for information and information system



FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of Federal Information and Information Systems

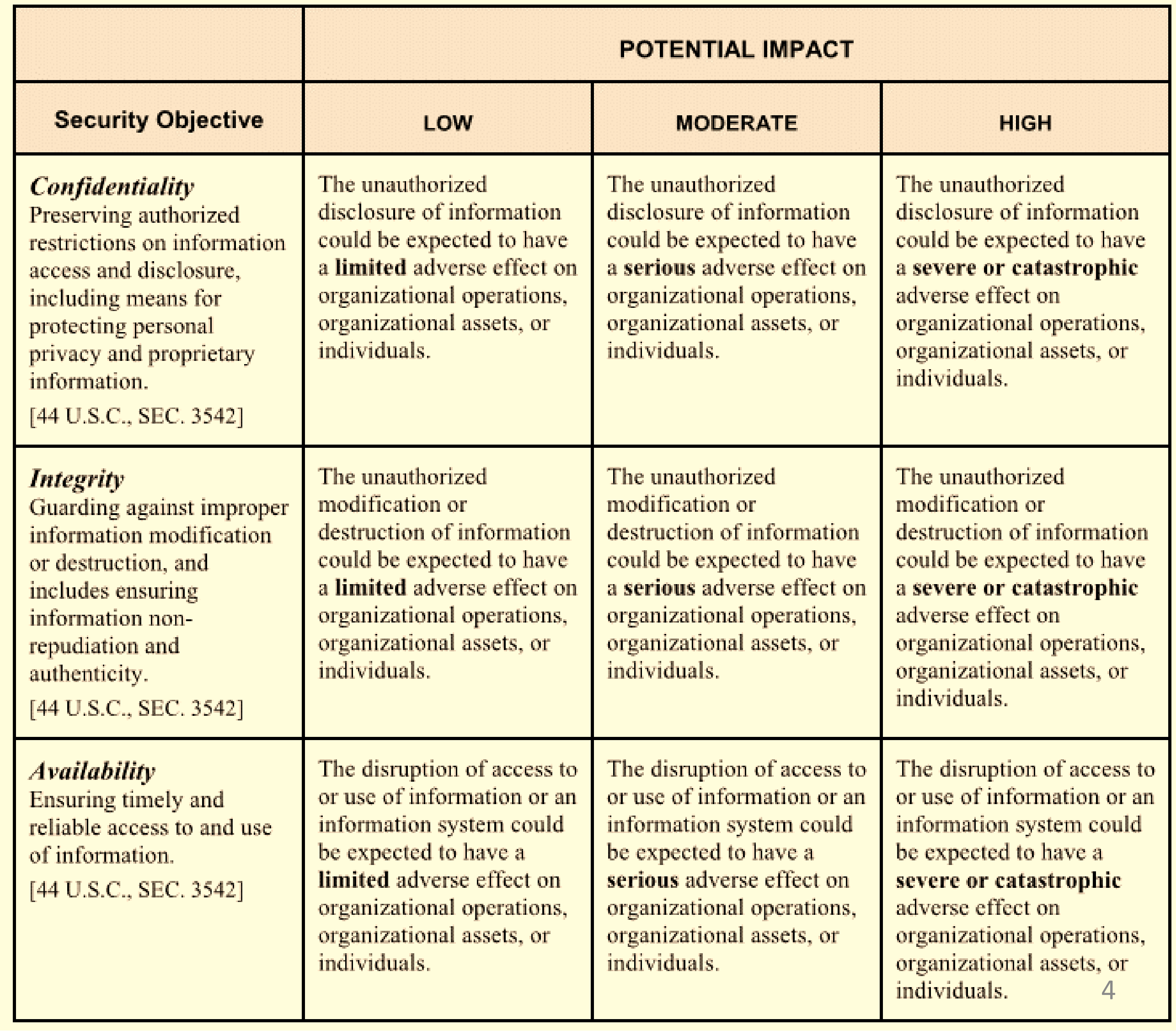
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

February 2004

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

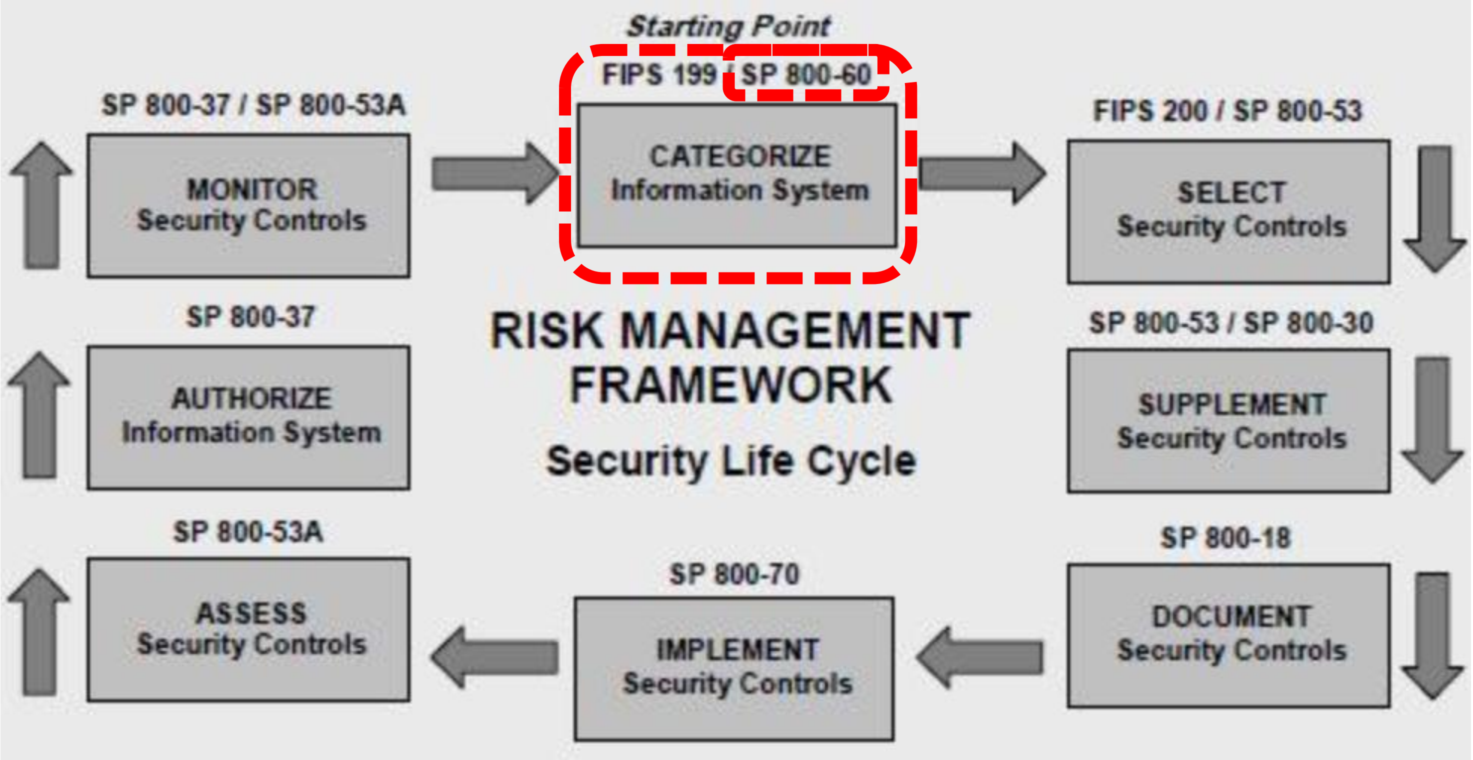
TECHNOLOGY ADMINISTRATION
Phillip J. Bond, Under Secretary for Technology

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

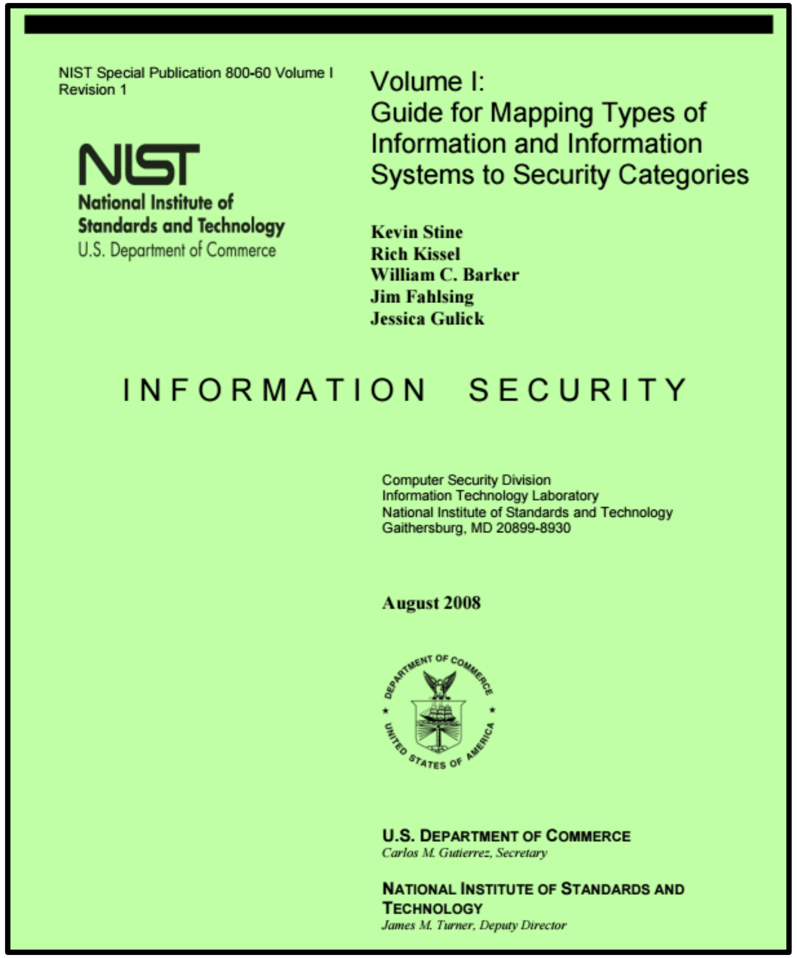


	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could 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.

Risk Management Framework



Mapping IS Types to Security Categories



NIST Special Publication 800-60 Volume I
Revision 1

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Volume I:
Guide for Mapping Types of Information and Information Systems to Security Categories

Kevin Stine
Rich Kissel
William C. Barker
Jim Fahlsing
Jessica Gulick

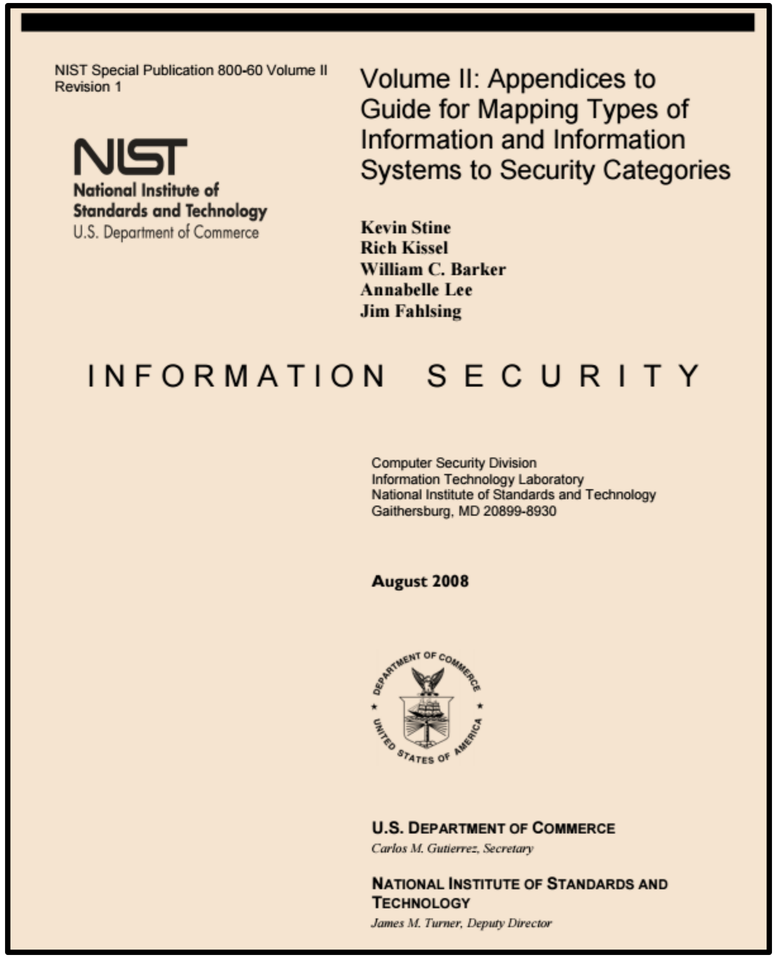
INFORMATION SECURITY

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

August 2008

U.S. DEPARTMENT OF COMMERCE
Carlos M. Gutierrez, Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
James M. Turner, Deputy Director



NIST Special Publication 800-60 Volume II
Revision 1

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Volume II: Appendices to
Guide for Mapping Types of Information and Information Systems to Security Categories

Kevin Stine
Rich Kissel
William C. Barker
Annabelle Lee
Jim Fahlsing

INFORMATION SECURITY

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

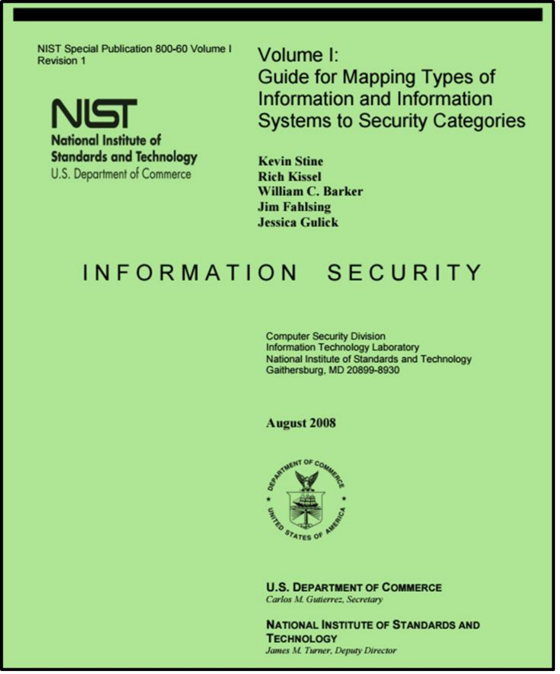
August 2008

U.S. DEPARTMENT OF COMMERCE
Carlos M. Gutierrez, Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
James M. Turner, Deputy Director

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v2r1.pdf



NIST Special Publication 800-60 Volume I
Revision 1

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Volume I:
Guide for Mapping Types of
Information and Information
Systems to Security Categories

Kevin Stine
Rich Kissel
William C. Barker
Jim Fahlsing
Jessica Gulick

INFORMATION SECURITY

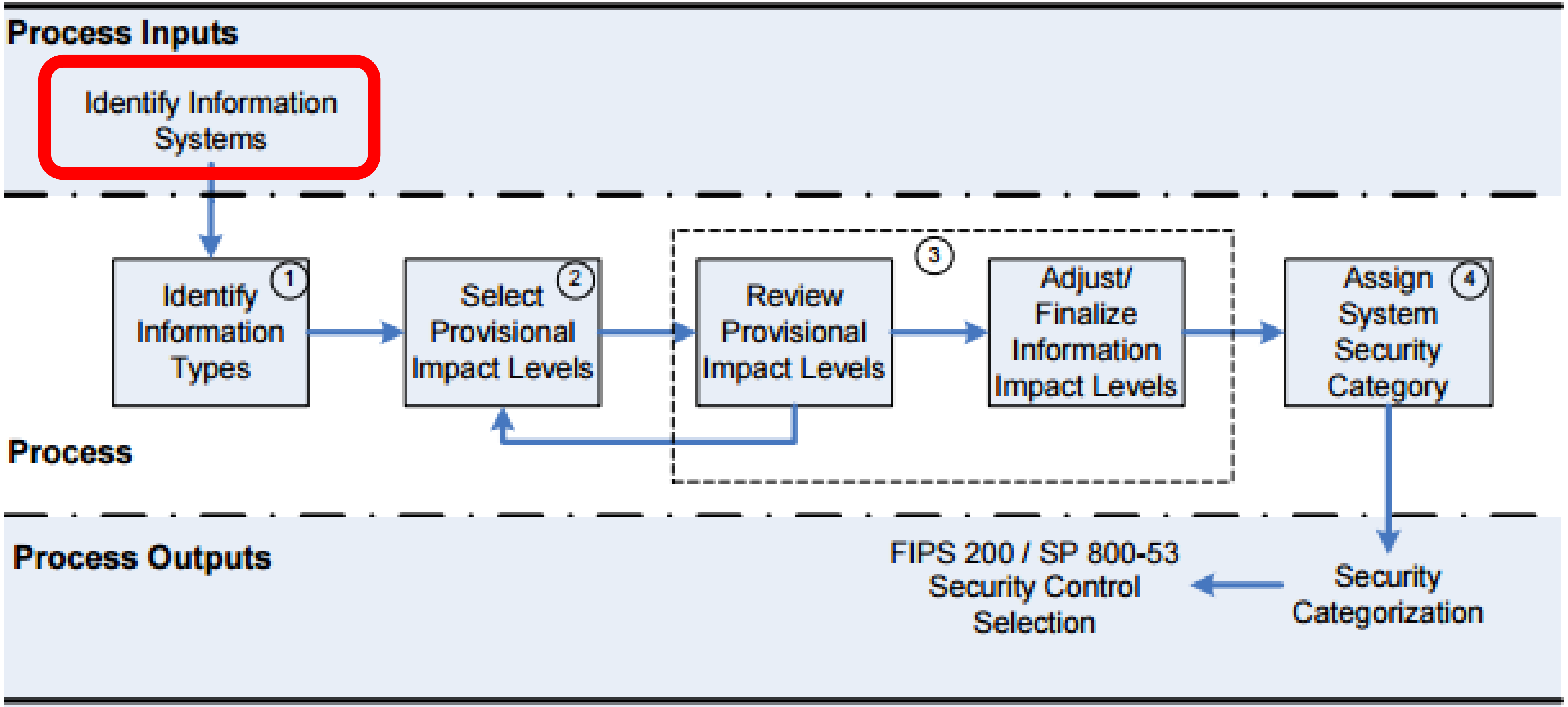
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

August 2008

U.S. DEPARTMENT OF COMMERCE
Carlos M. Gutierrez, Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
James M. Turner, Deputy Director

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf



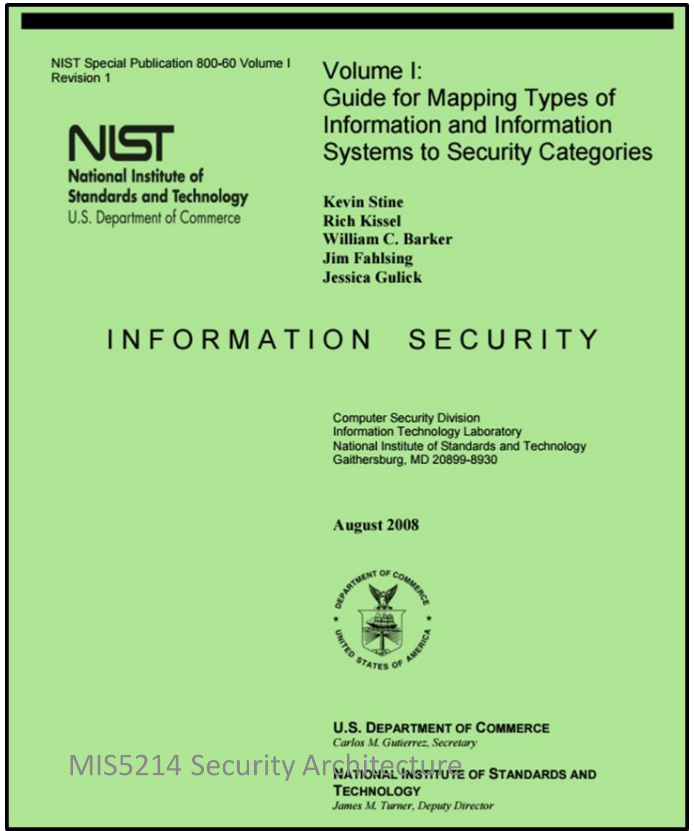
Process Inputs
Identify Information Systems
Identify Information Types
1
Select Provisional Impact Levels
2
Review Provisional Impact Levels
3
Adjust/ Finalize Information Impact Levels
Assign System Security Category
4
Process
Process Outputs
FIPS 200 / SP 800-53 Security Control Selection
Security Categorization

Figure 2: SP 800-60 Security Categorization Process Execution

2 Broad types of Information and Information Systems

1. **Mission-based Information & Information Systems**

2. Management and Support Information & Information Systems



NIST Special Publication 800-60 Volume I
Revision 1

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Volume I:
Guide for Mapping Types of Information and Information Systems to Security Categories

Kevin Stine
Rich Kissel
William C. Barker
Jim Fahlsing
Jessica Gulick

INFORMATION SECURITY

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

August 2008

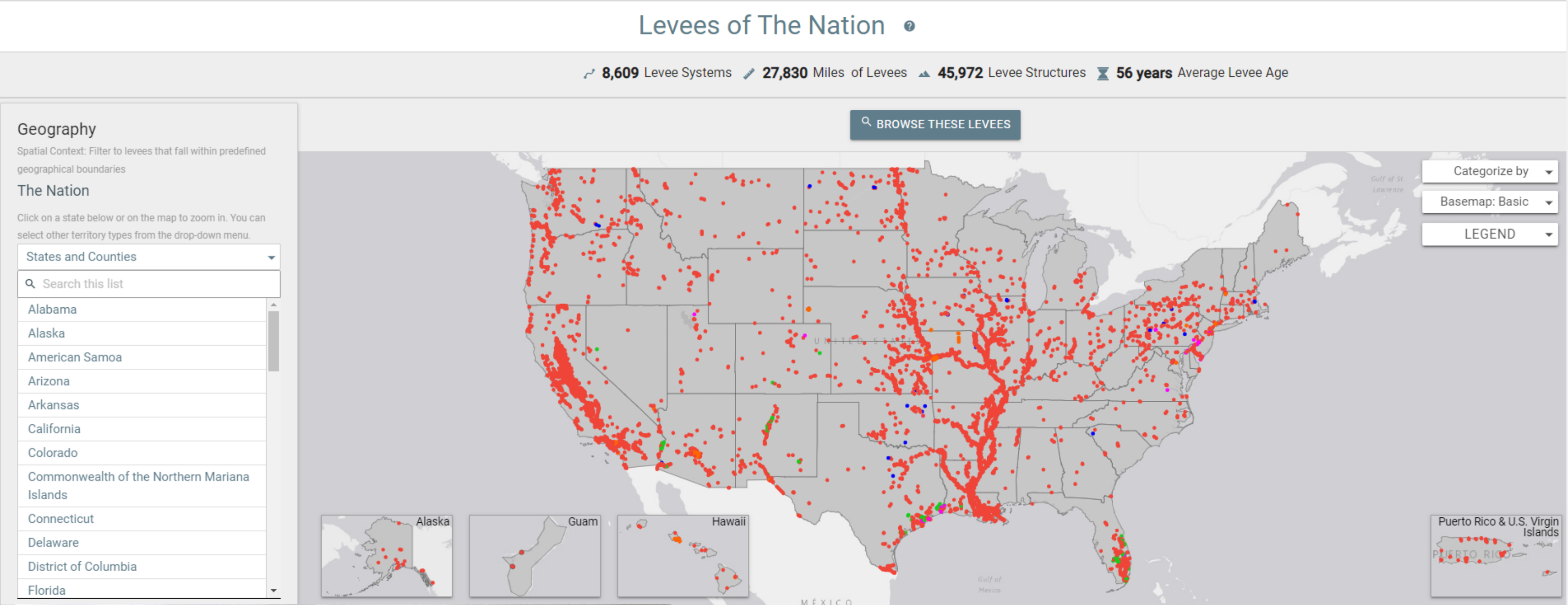
U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology
James M. Turner, Deputy Director

Mission-based Information and Information Systems

1. Defense and National Security
2. Homeland Security
3. Intelligence Operations
4. Disaster Management
5. International Affairs and Commerce
6. Natural Resources
7. Energy
8. Environmental Management
9. Economic Development
10. Community and Social Services
11. Transportation
12. Education
13. Workforce Management
14. Health
15. Income Security
16. Law Enforcement
17. Litigation and Judicial Activities
18. Federal Correctional Activities
19. General Sciences and Innovation
20. Knowledge Creation and Management
21. Regulatory Compliance and Enforcement
22. Public Goods Creation and Management
23. Federal Financial Assistance
24. Credit and Insurance
25. Transfers to State/Local Governments
26. Direct Services for Citizens

Disaster Management Information System Example



Levees of The Nation

8,609 Levee Systems 27,830 Miles of Levees 45,972 Levee Structures 56 years Average Levee Age

Geography

Spatial Context: Filter to levees that fall within predefined geographical boundaries

The Nation

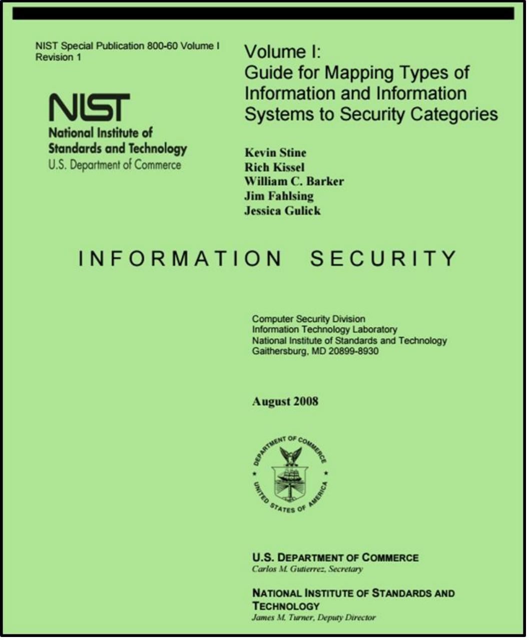
Click on a state below or on the map to zoom in. You can select other territory types from the drop-down menu.

States and Counties

Search this list

- Alabama
- Alaska
- American Samoa
- Arizona
- Arkansas
- California
- Colorado
- Commonwealth of the Northern Mariana Islands
- Connecticut
- Delaware
- District of Columbia
- Florida

2 Broad Types of Information and Information Systems



NIST Special Publication 800-60 Volume I
Revision 1

Volume I:
Guide for Mapping Types of Information and Information Systems to Security Categories

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Kevin Stine
Rich Kissel
William C. Barker
Jim Fahlsing
Jessica Gulick

INFORMATION SECURITY

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

August 2008

U.S. DEPARTMENT OF COMMERCE
Carlos M. Gutierrez, Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
James M. Turner, Deputy Director

1. Mission-based Information & Information Systems

2. **Management and Support Information & Information Systems**

    i. **Services Delivery Support Functions**

    ii. **Government Resource Management Functions**

Services Delivery Support Functions and Information Types

1. Controls and Oversight
2. Regulatory Development
3. Planning and Budgeting
4. Internal Risk Management and Mitigation
5. Revenue Collection
6. Public Affairs
7. Legislative Relations
8. General Government

Example Management & Support Information & Information Systems

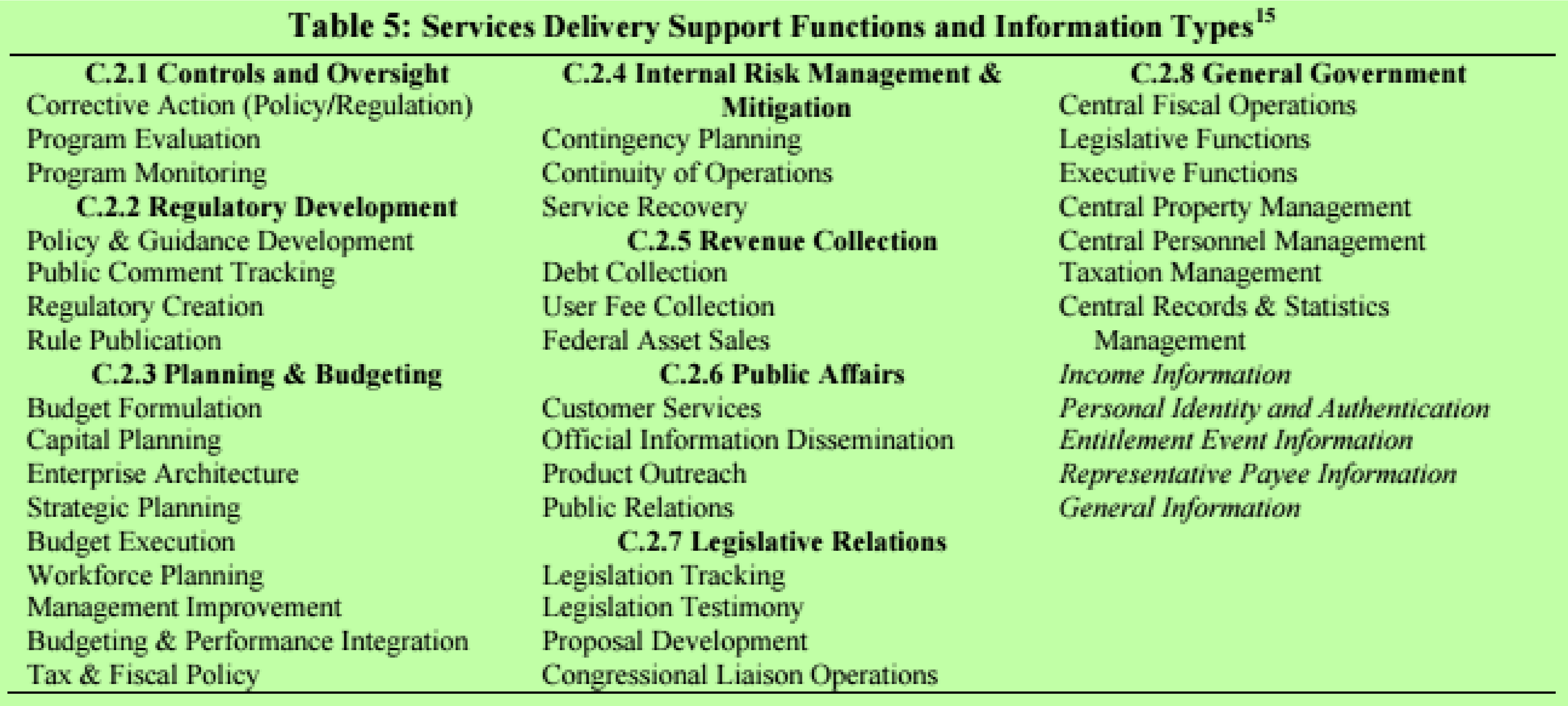


Table 5: Services Delivery Support Functions and Information Types[15]

C.2.1 Controls and Oversight

Corrective Action (Policy/Regulation)
Program Evaluation
Program Monitoring

C.2.2 Regulatory Development

Policy & Guidance Development
Public Comment Tracking
Regulatory Creation
Rule Publication

C.2.3 Planning & Budgeting

Budget Formulation
Capital Planning
Enterprise Architecture
Strategic Planning
Budget Execution
Workforce Planning
Management Improvement
Budgeting & Performance Integration
Tax & Fiscal Policy

C.2.4 Internal Risk Management & Mitigation

Contingency Planning
Continuity of Operations
Service Recovery

C.2.5 Revenue Collection

Debt Collection
User Fee Collection
Federal Asset Sales

C.2.6 Public Affairs

Customer Services
Official Information Dissemination
Product Outreach
Public Relations

C.2.7 Legislative Relations

Legislation Tracking
Legislation Testimony
Proposal Development
Congressional Liaison Operations

C.2.8 General Government

Central Fiscal Operations
Legislative Functions
Executive Functions
Central Property Management
Central Personnel Management
Taxation Management
Central Records & Statistics Management
Income Information
Personal Identity and Authentication
Entitlement Event Information
Representative Payee Information
General Information

Example Resource Management Functions & Information Types

1. Administrative Management
2. Financial Management
3. Human Resources Management
4. Supply Chain Management
5. Information and Technology Management

Example Management and Support Information and Information Systems

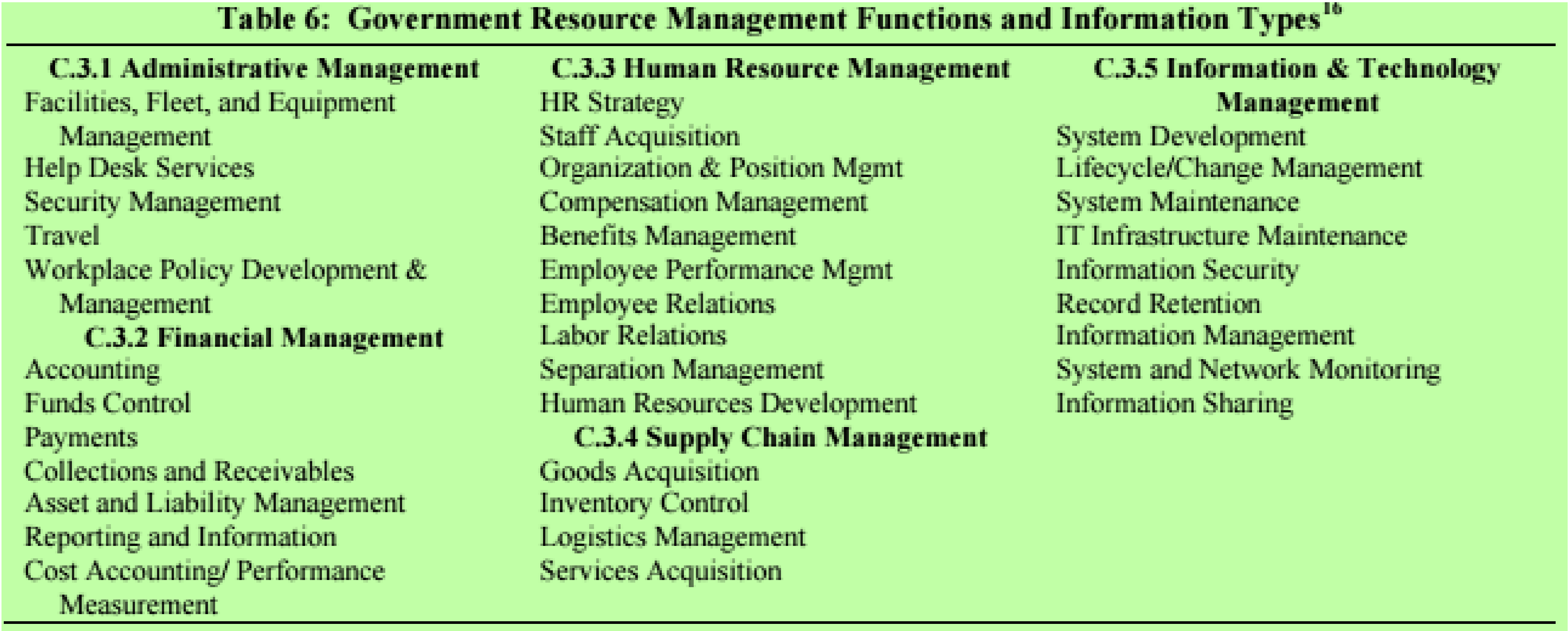


Table 6: Government Resource Management Functions and Information Types[16]

C.3.1 Administrative Management

Facilities, Fleet, and Equipment Management
Help Desk Services
Security Management
Travel
Workplace Policy Development & Management

C.3.2 Financial Management

Accounting
Funds Control
Payments
Collections and Receivables
Asset and Liability Management
Reporting and Information
Cost Accounting/ Performance Measurement

C.3.3 Human Resource Management

HR Strategy
Staff Acquisition
Organization & Position Mgmt
Compensation Management
Benefits Management
Employee Performance Mgmt
Employee Relations
Labor Relations
Separation Management
Human Resources Development

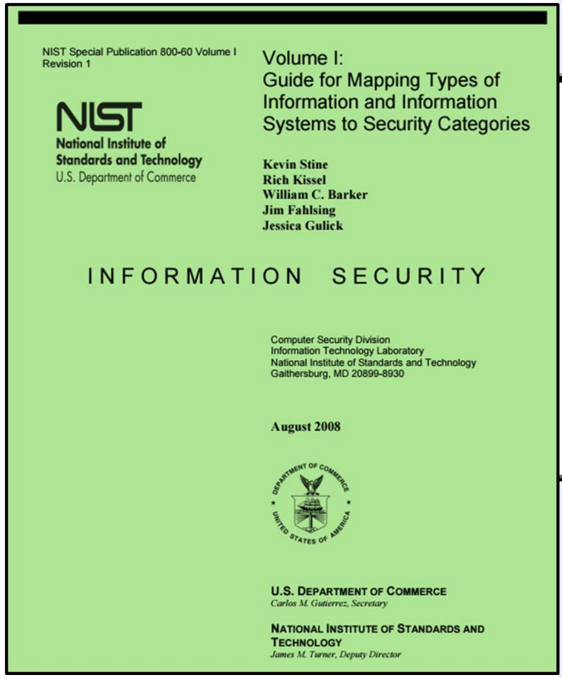
C.3.4 Supply Chain Management

Goods Acquisition
Inventory Control
Logistics Management
Services Acquisition

C.3.5 Information & Technology Management

System Development
Lifecycle/Change Management
System Maintenance
IT Infrastructure Maintenance
Information Security
Record Retention
Information Management
System and Network Monitoring
Information Sharing

1. Identify Information Types



NIST Special Publication 800-60 Volume I
Revision 1

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Volume I:
Guide for Mapping Types of Information and Information Systems to Security Categories

Kevin Stine
Rich Kissel
William C. Barker
Jim Fahlsing
Jessica Gulick

INFORMATION SECURITY

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

August 2008

U.S. DEPARTMENT OF COMMERCE
Carlos M. Gutierrez, Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
James M. Turner, Deputy Director

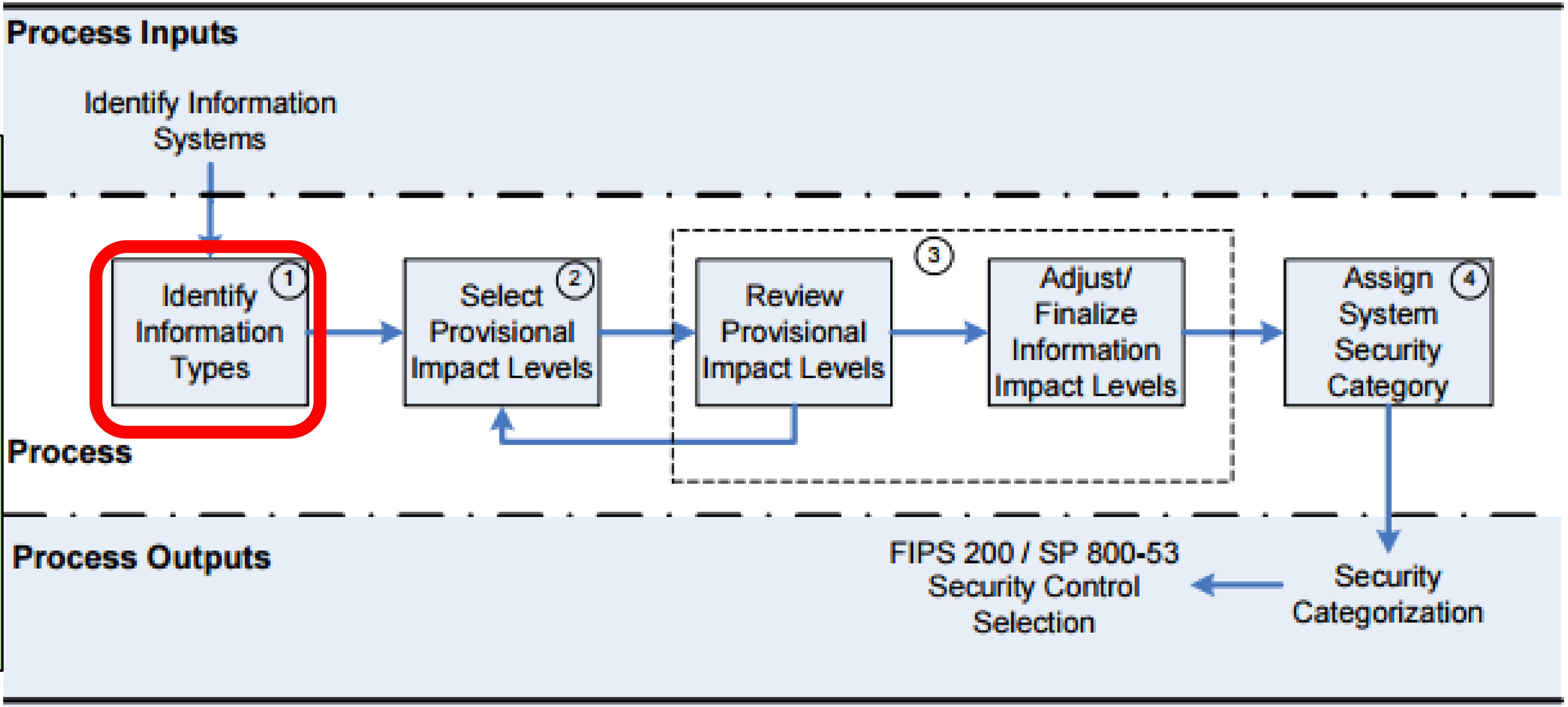
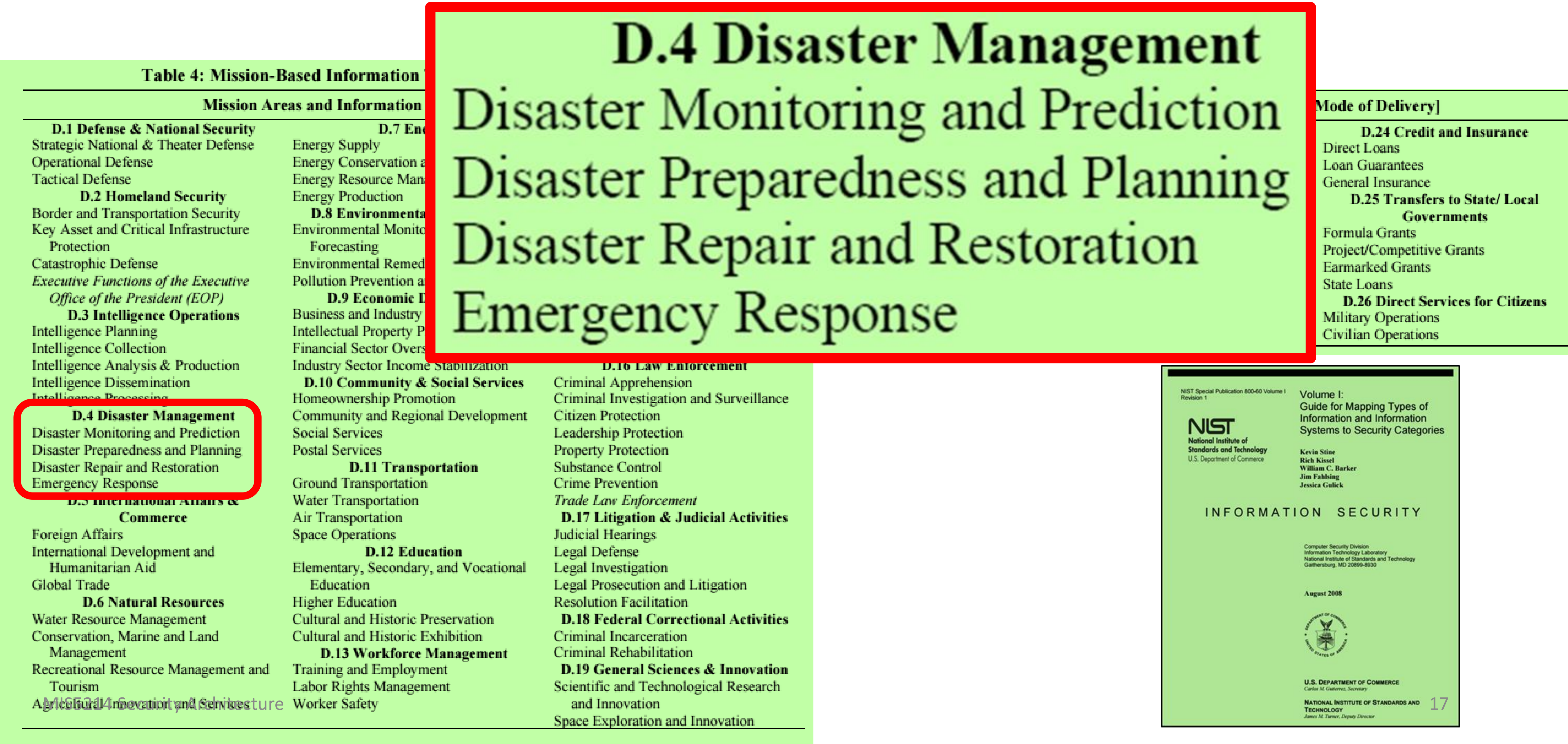

Process Inputs
Identify Information Systems
Identify Information Types 1
Select Provisional Impact Levels 2
3
Review Provisional Impact Levels
Adjust/ Finalize Information Impact Levels
Assign System Security Category 4
Process
Process Outputs
FIPS 200 / SP 800-53 Security Control Selection
Security Categorization

Figure 2: SP 800-60 Security Categorization Process Execution

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf

Disaster Management Information Types



D.4 Disaster Management

Disaster Monitoring and Prediction

Disaster Preparedness and Planning

Disaster Repair and Restoration

Emergency Response

Table 4: Mission-Based Information

Mission Areas and Information

D.1 Defense & National Security
Strategic National & Theater Defense
Operational Defense
Tactical Defense
D.2 Homeland Security
Border and Transportation Security
Key Asset and Critical Infrastructure Protection
Catastrophic Defense
Executive Functions of the Executive Office of the President (EOP)
D.3 Intelligence Operations
Intelligence Planning
Intelligence Collection
Intelligence Analysis & Production
Intelligence Dissemination
Intelligence Processing
D.4 Disaster Management
Disaster Monitoring and Prediction
Disaster Preparedness and Planning
Disaster Repair and Restoration
Emergency Response
D.5 International Affairs & Commerce
Foreign Affairs
International Development and Humanitarian Aid
Global Trade
D.6 Natural Resources
Water Resource Management
Conservation, Marine and Land Management
Recreational Resource Management and Tourism
Agricultural Innovation and Services

D.7 En
Energy Supply
Energy Conservation a
Energy Resource Man
Energy Production
D.8 Environmenta
Environmental Monito
Forecasting
Environmental Remed
Pollution Prevention a
D.9 Economic D
Business and Industry
Intellectual Property P
Financial Sector Overs
Industry Sector Income Stabilization
D.10 Community & Social Services
Homeownership Promotion
Community and Regional Development
Social Services
Postal Services
D.11 Transportation
Ground Transportation
Water Transportation
Air Transportation
Space Operations
D.12 Education
Elementary, Secondary, and Vocational Education
Higher Education
Cultural and Historic Preservation
Cultural and Historic Exhibition
D.13 Workforce Management
Training and Employment
Labor Rights Management
Worker Safety

D.16 Law Enforcement
Criminal Apprehension
Criminal Investigation and Surveillance
Citizen Protection
Leadership Protection
Property Protection
Substance Control
Crime Prevention
Trade Law Enforcement
D.17 Litigation & Judicial Activities
Judicial Hearings
Legal Defense
Legal Investigation
Legal Prosecution and Litigation
Resolution Facilitation
D.18 Federal Correctional Activities
Criminal Incarceration
Criminal Rehabilitation
D.19 General Sciences & Innovation
Scientific and Technological Research and Innovation
Space Exploration and Innovation

Mode of Delivery]

D.24 Credit and Insurance
Direct Loans
Loan Guarantees
General Insurance
D.25 Transfers to State/ Local Governments
Formula Grants
Project/Competitive Grants
Earmarked Grants
State Loans
D.26 Direct Services for Citizens
Military Operations
Civilian Operations

NIST Special Publication 800-60 Volume I Revision 1

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Volume I:
Guide for Mapping Types of Information and Information Systems to Security Categories

Kevin Stine
Rich Kissel
William C. Barker
Jim Fahlsing
Jessica Gulick

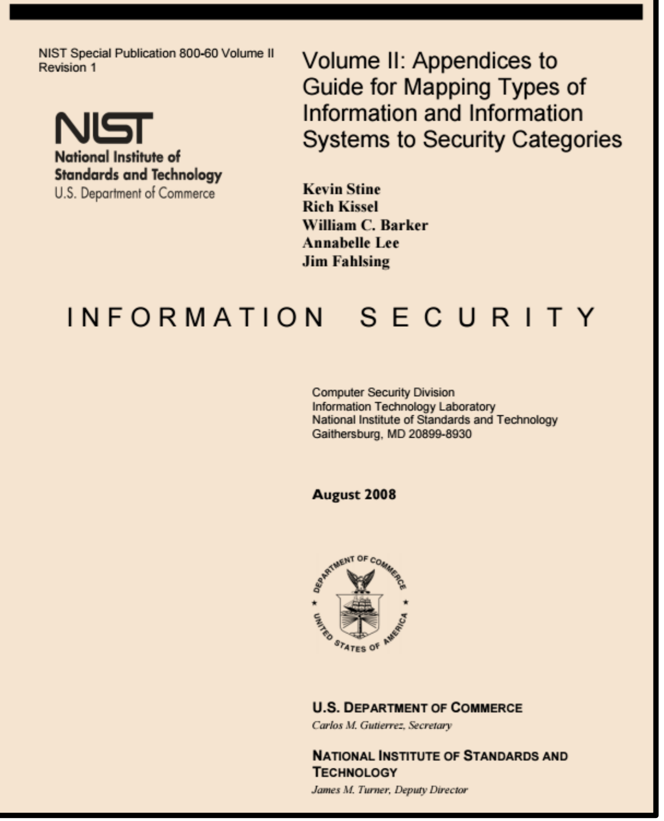
INFORMATION SECURITY

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

August 2008

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology
James M. Turner, Deputy Director



NIST Special Publication 800-60 Volume II Revision 1

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories

Kevin Stine
Rich Kissel
William C. Barker
Annabelle Lee
Jim Fahlsing

INFORMATION SECURITY

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

August 2008

U.S. DEPARTMENT OF COMMERCE
Carlos M. Gutierrez, Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
James M. Turner, Deputy Director

2. Select Provisional Impact Levels for the identified information system

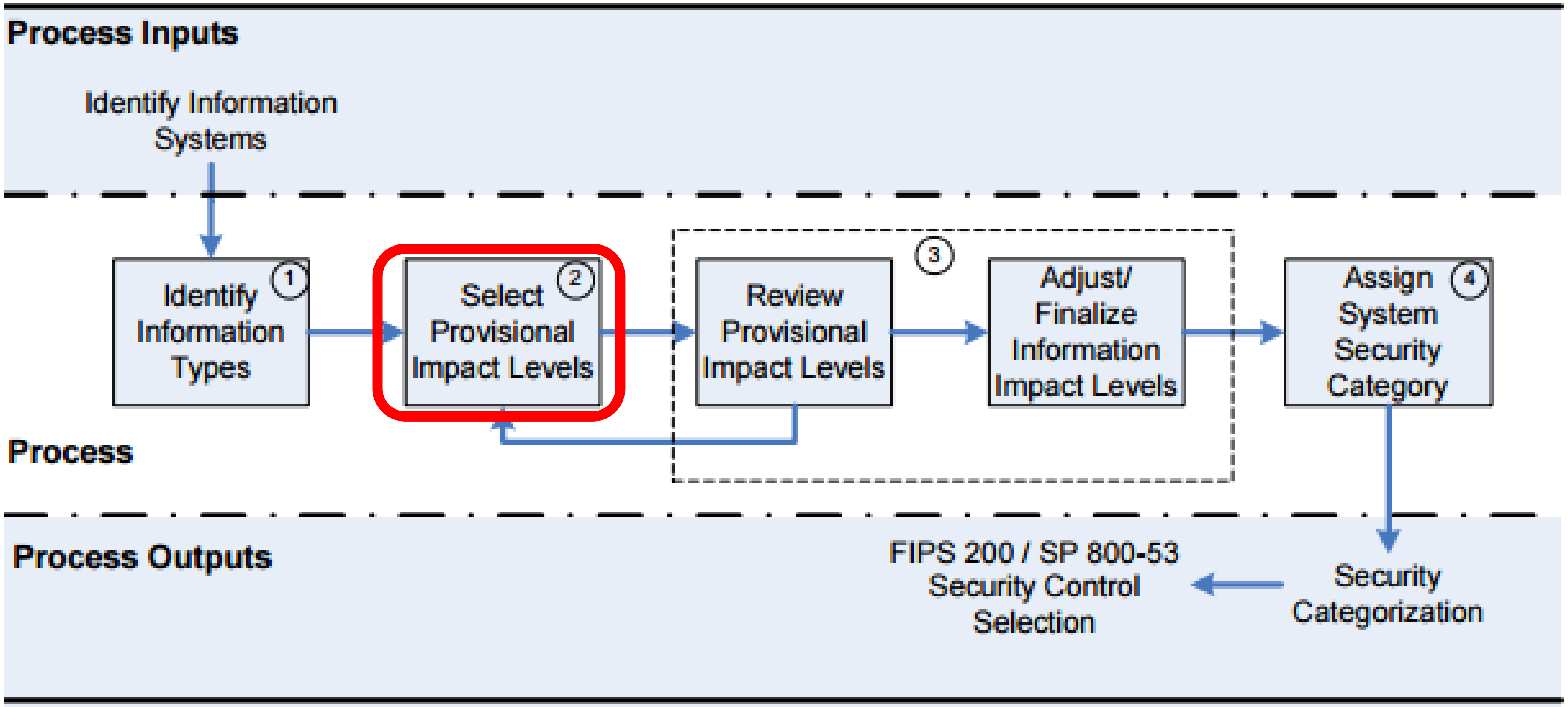
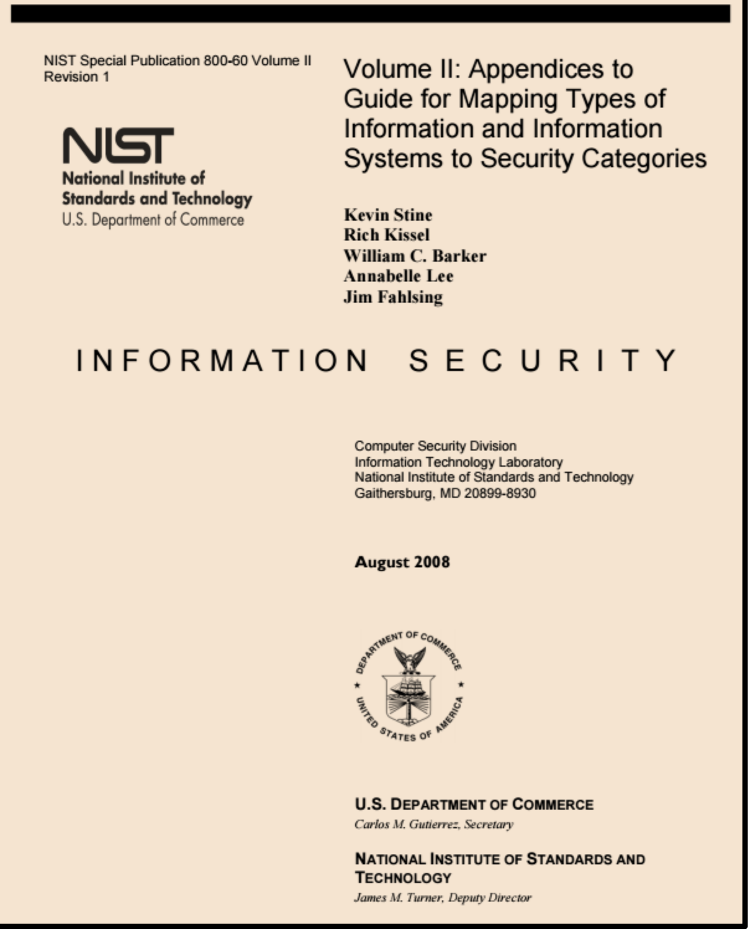

Process Inputs
Identify Information Systems
Identify Information Types
1
Select Provisional Impact Levels
2
3
Review Provisional Impact Levels
Adjust/ Finalize Information Impact Levels
Assign System Security Category
4
Process
Process Outputs
FIPS 200 / SP 800-53 Security Control Selection
Security Categorization

Figure 2: SP 800-60 Security Categorization Process Execution



NIST Special Publication 800-60 Volume II
Revision 1

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories

Kevin Stine
Rich Kissel
William C. Barker
Annabelle Lee
Jim Fahlsing

INFORMATION SECURITY

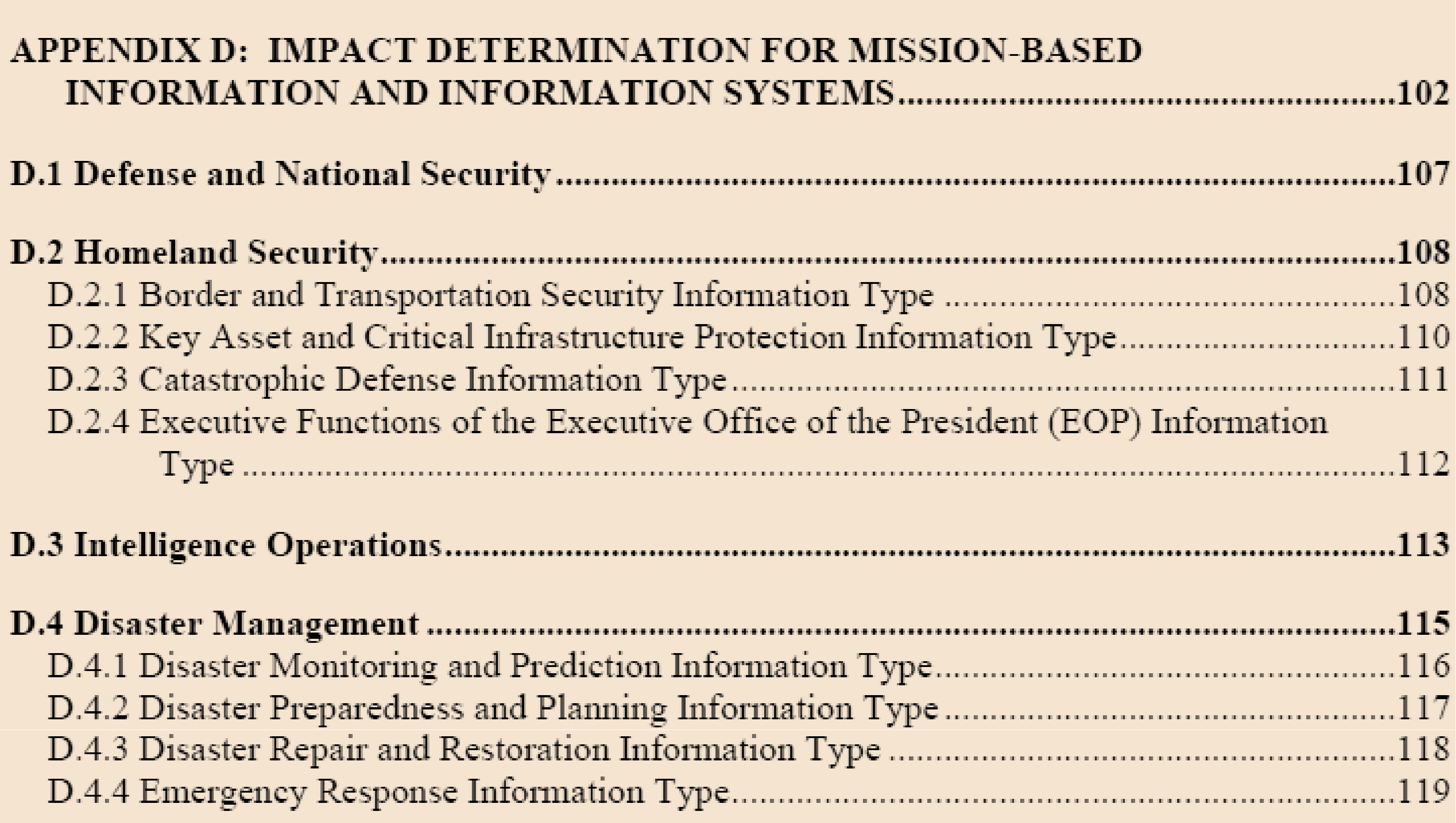
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

August 2008

U.S. DEPARTMENT OF COMMERCE
Carlos M. Gutierrez, Secretary

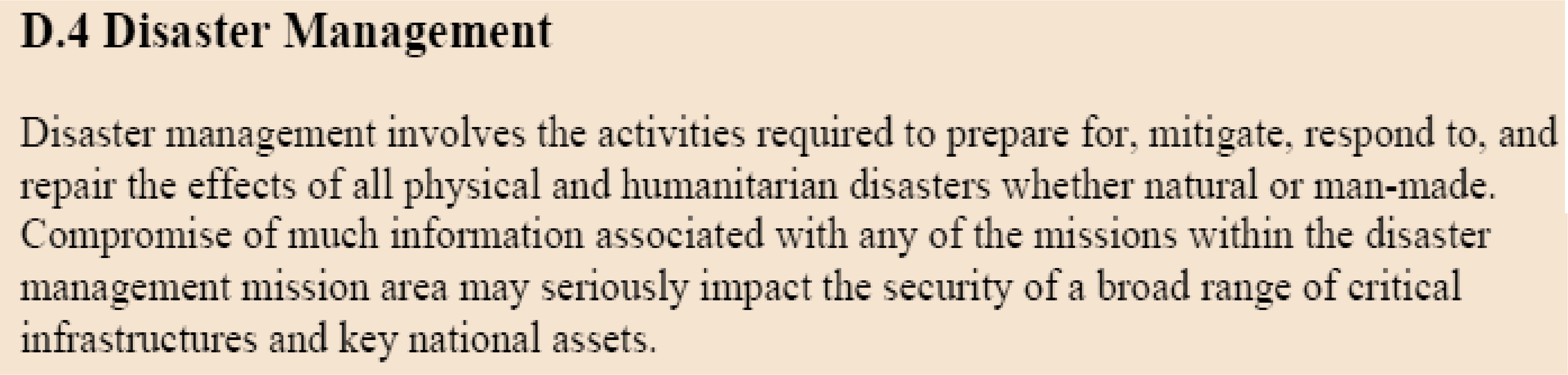
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
James M. Turner, Deputy Director

Disaster Management Information Types



https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v2r1.pdf

Disaster Management Information Impact

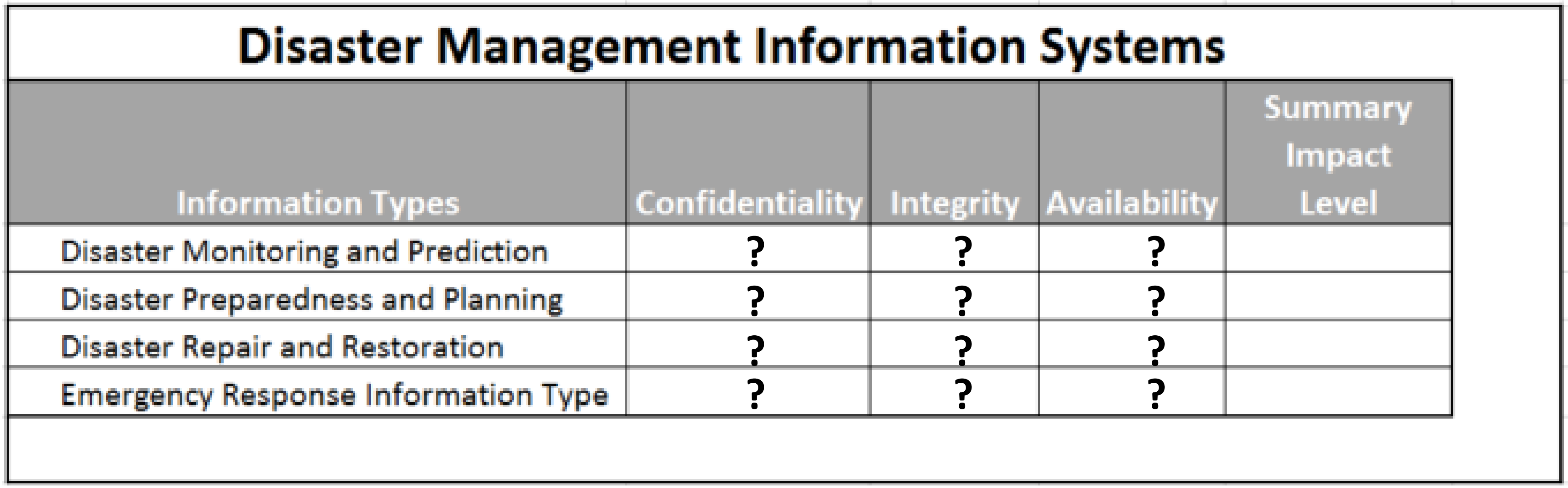


D.4 Disaster Management

Disaster management involves the activities required to prepare for, mitigate, respond to, and repair the effects of all physical and humanitarian disasters whether natural or man-made. Compromise of much information associated with any of the missions within the disaster management mission area may seriously impact the security of a broad range of critical infrastructures and key national assets.

Can you use…

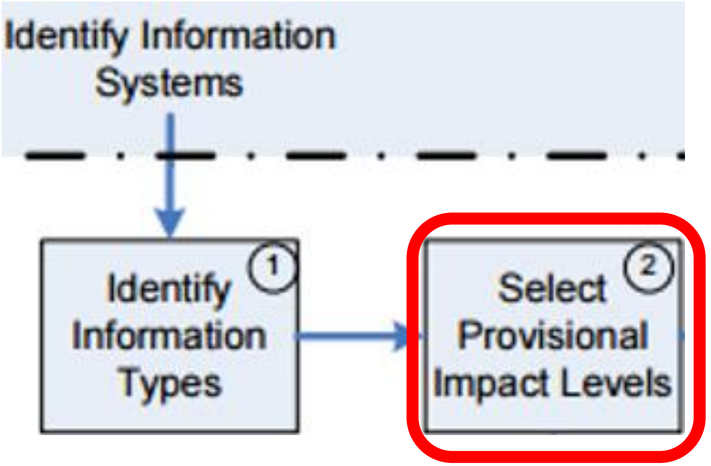
- *NIST SP 800-60 V.2 R1 to determine the Impact Levels for the Disaster Information Types ?*

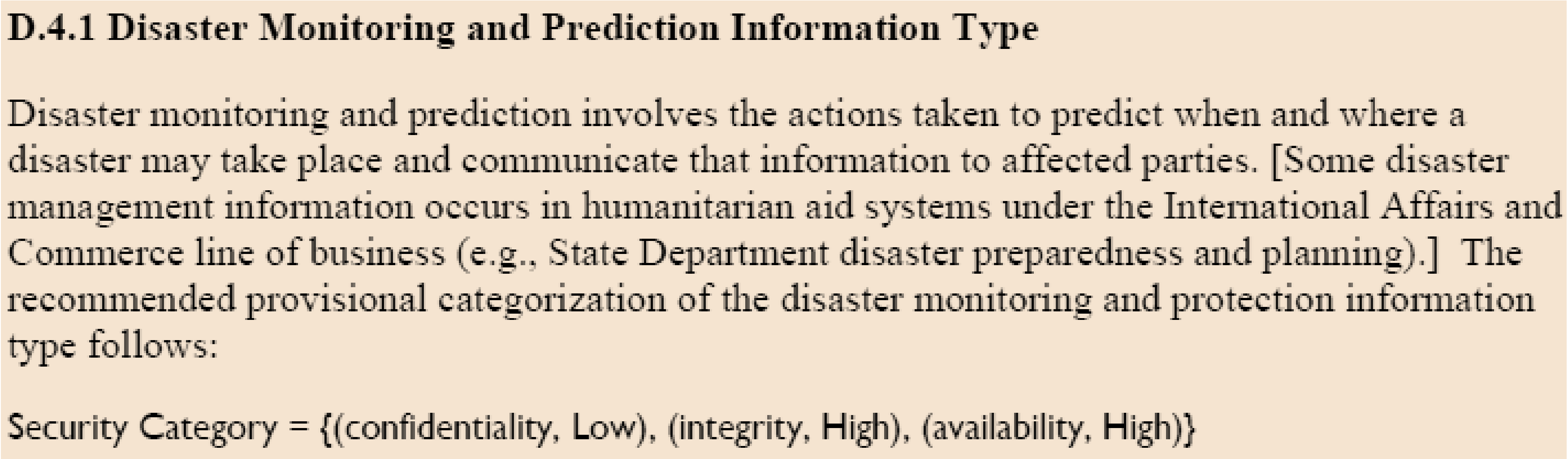


Disaster Management Information Systems

Information Types	Confidentiality	Integrity	Availability	Summary Impact Level
Disaster Monitoring and Prediction	?	?	?	
Disaster Preparedness and Planning	?	?	?	
Disaster Repair and Restoration	?	?	?	
Emergency Response Information Type	?	?	?	

Disaster Management Information Types

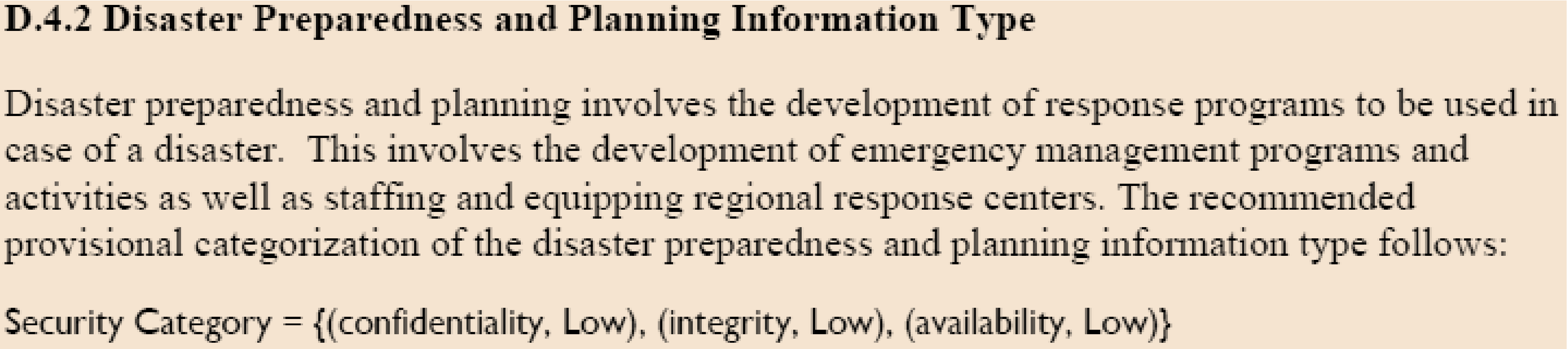

Identify Information Systems
1
Identify Information Types
2
Select Provisional Impact Levels



D.4.1 Disaster Monitoring and Prediction Information Type

Disaster monitoring and prediction involves the actions taken to predict when and where a disaster may take place and communicate that information to affected parties. [Some disaster management information occurs in humanitarian aid systems under the International Affairs and Commerce line of business (e.g., State Department disaster preparedness and planning).] The recommended provisional categorization of the disaster monitoring and protection information type follows:

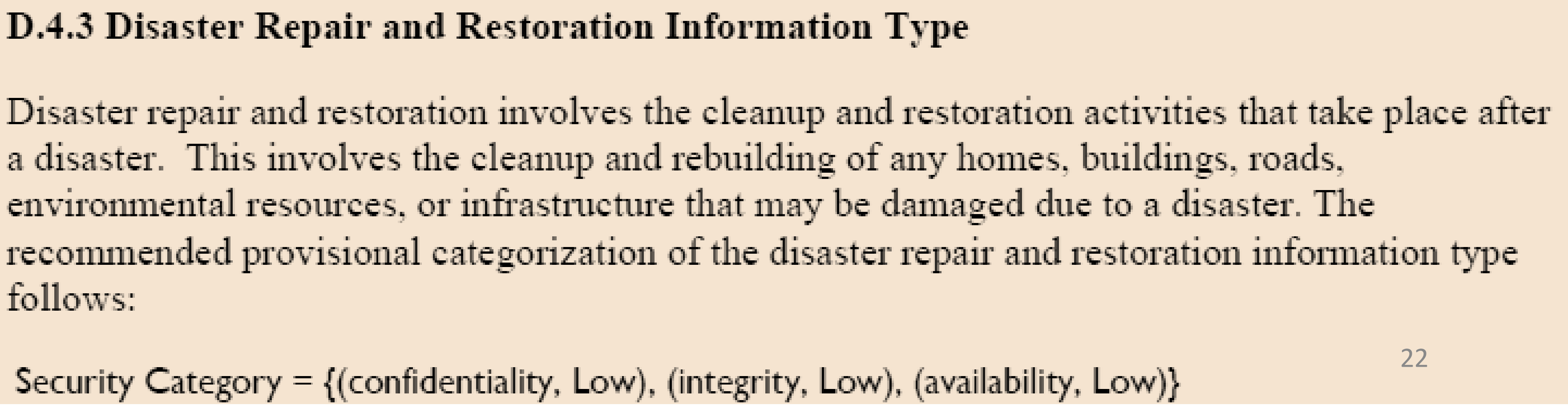
Security Category = {(confidentiality, Low), (integrity, High), (availability, High)}



D.4.2 Disaster Preparedness and Planning Information Type

Disaster preparedness and planning involves the development of response programs to be used in case of a disaster. This involves the development of emergency management programs and activities as well as staffing and equipping regional response centers. The recommended provisional categorization of the disaster preparedness and planning information type follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

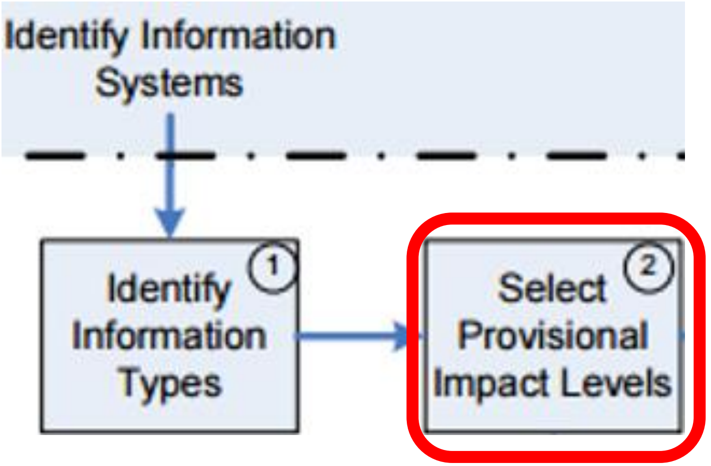


D.4.3 Disaster Repair and Restoration Information Type

Disaster repair and restoration involves the cleanup and restoration activities that take place after a disaster. This involves the cleanup and rebuilding of any homes, buildings, roads, environmental resources, or infrastructure that may be damaged due to a disaster. The recommended provisional categorization of the disaster repair and restoration information type follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

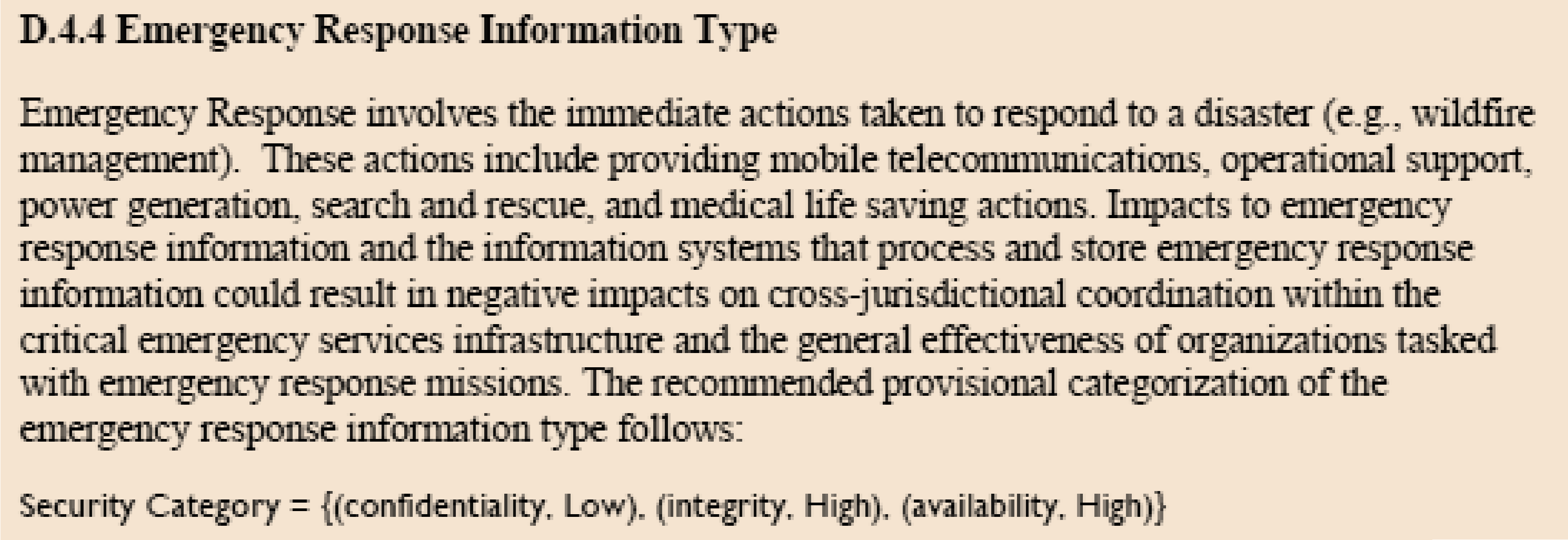
Disaster Management Information Types



Identify Information Systems

Identify Information Types ①

Select Provisional Impact Levels ②



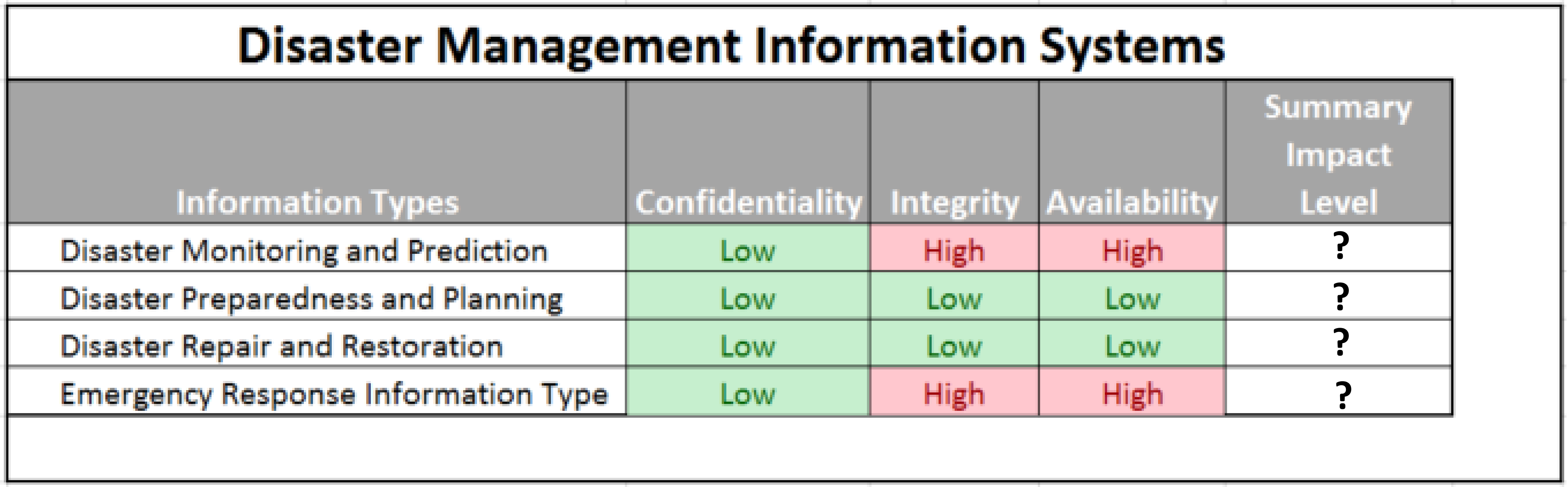
D.4.4 Emergency Response Information Type

Emergency Response involves the immediate actions taken to respond to a disaster (e.g., wildfire management). These actions include providing mobile telecommunications, operational support, power generation, search and rescue, and medical life saving actions. Impacts to emergency response information and the information systems that process and store emergency response information could result in negative impacts on cross-jurisdictional coordination within the critical emergency services infrastructure and the general effectiveness of organizations tasked with emergency response missions. The recommended provisional categorization of the emergency response information type follows:

Security Category = {(confidentiality, Low), (integrity, High), (availability, High)}

Question

- *Can you determine Summary Impact Levels for Disaster Information Types ?*

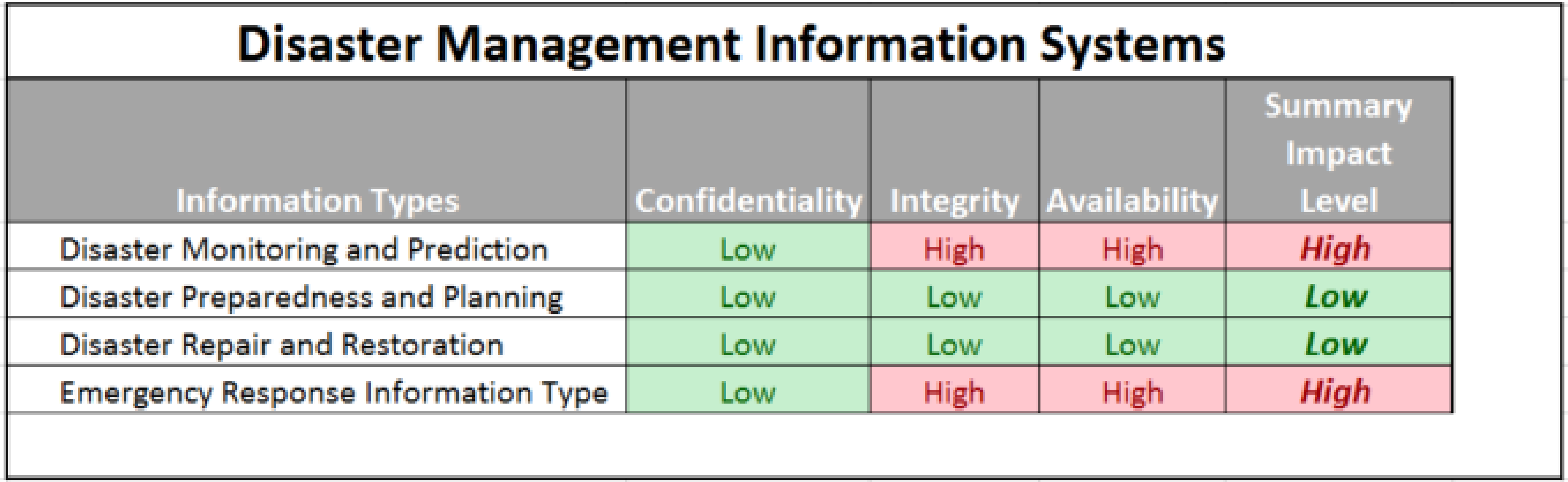


Disaster Management Information Systems

Information Types	Confidentiality	Integrity	Availability	Summary Impact Level
Disaster Monitoring and Prediction	Low	High	High	?
Disaster Preparedness and Planning	Low	Low	Low	?
Disaster Repair and Restoration	Low	Low	Low	?
Emergency Response Information Type	Low	High	High	?

Answer…

- *Summary Impact Levels for the Disaster Information Types*

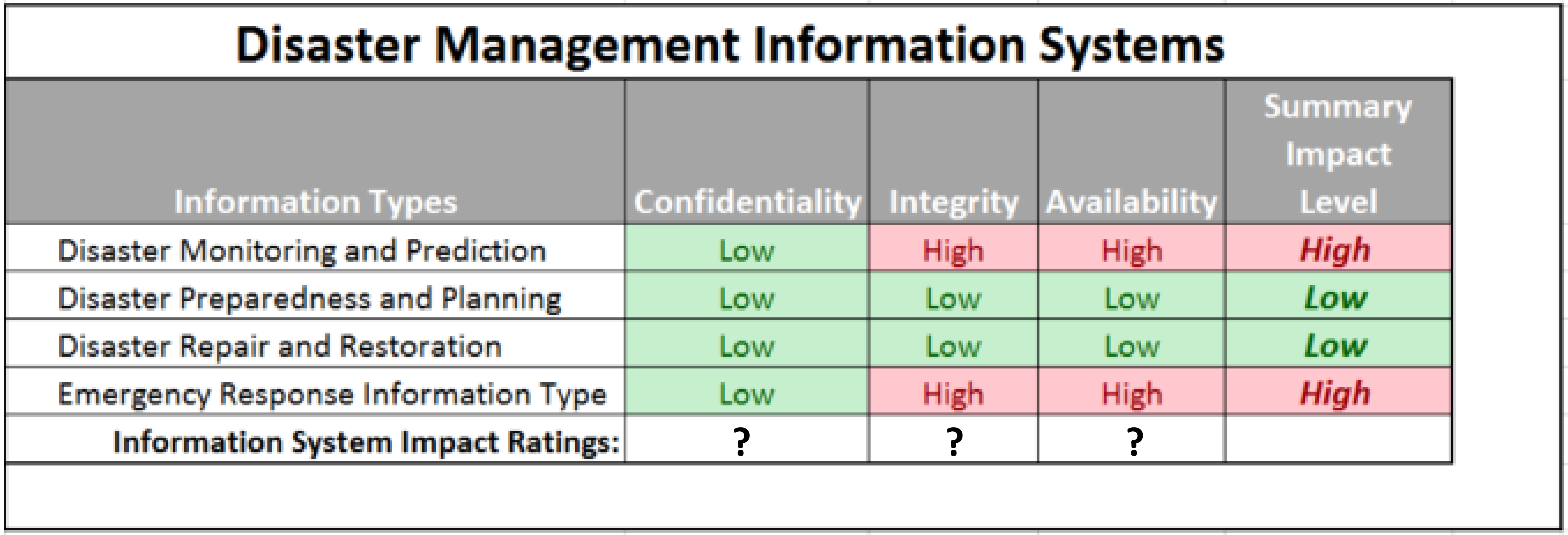


Disaster Management Information Systems

Information Types	Confidentiality	Integrity	Availability	Summary Impact Level
Disaster Monitoring and Prediction	Low	High	High	***High***
Disaster Preparedness and Planning	Low	Low	Low	***Low***
Disaster Repair and Restoration	Low	Low	Low	***Low***
Emergency Response Information Type	Low	High	High	***High***

Question -

- *Can you determine Overall Impact Levels for Disaster Information Types?*

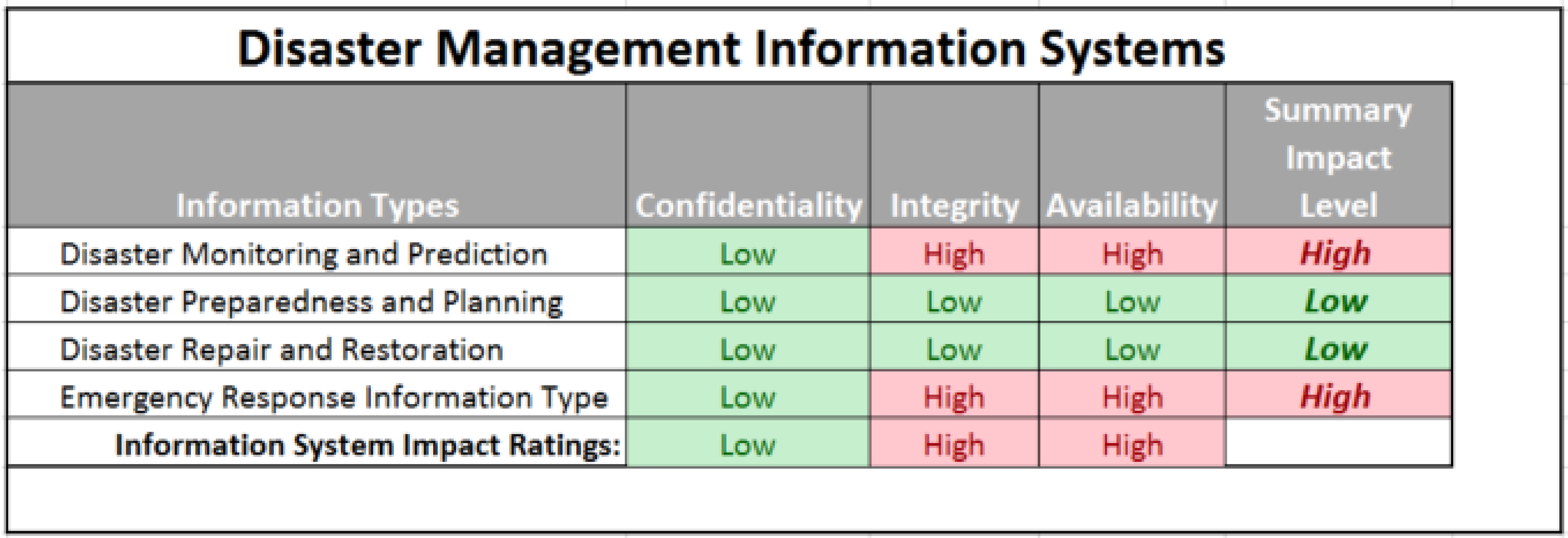


Disaster Management Information Systems

Information Types	Confidentiality	Integrity	Availability	Summary Impact Level
Disaster Monitoring and Prediction	Low	High	High	***High***
Disaster Preparedness and Planning	Low	Low	Low	***Low***
Disaster Repair and Restoration	Low	Low	Low	***Low***
Emergency Response Information Type	Low	High	High	***High***
Information System Impact Ratings:	**?**	**?**	**?**	

Answer

- *Overall Impact Levels for the Disaster Information Types*

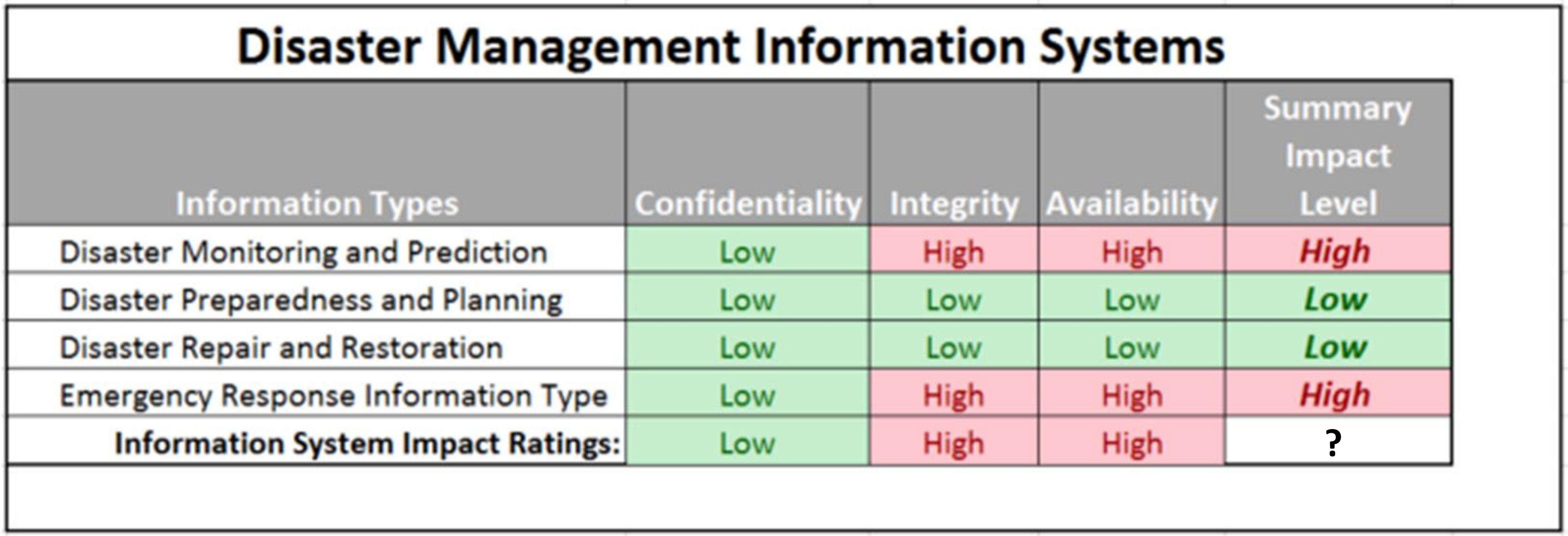


Disaster Management Information Systems

Information Types	Confidentiality	Integrity	Availability	Summary Impact Level
Disaster Monitoring and Prediction	Low	High	High	***High***
Disaster Preparedness and Planning	Low	Low	Low	***Low***
Disaster Repair and Restoration	Low	Low	Low	***Low***
Emergency Response Information Type	Low	High	High	***High***
Information System Impact Ratings:	Low	High	High	

Question

- *Can you determine overall Impact Level of a system of Disaster Information Systems ?*

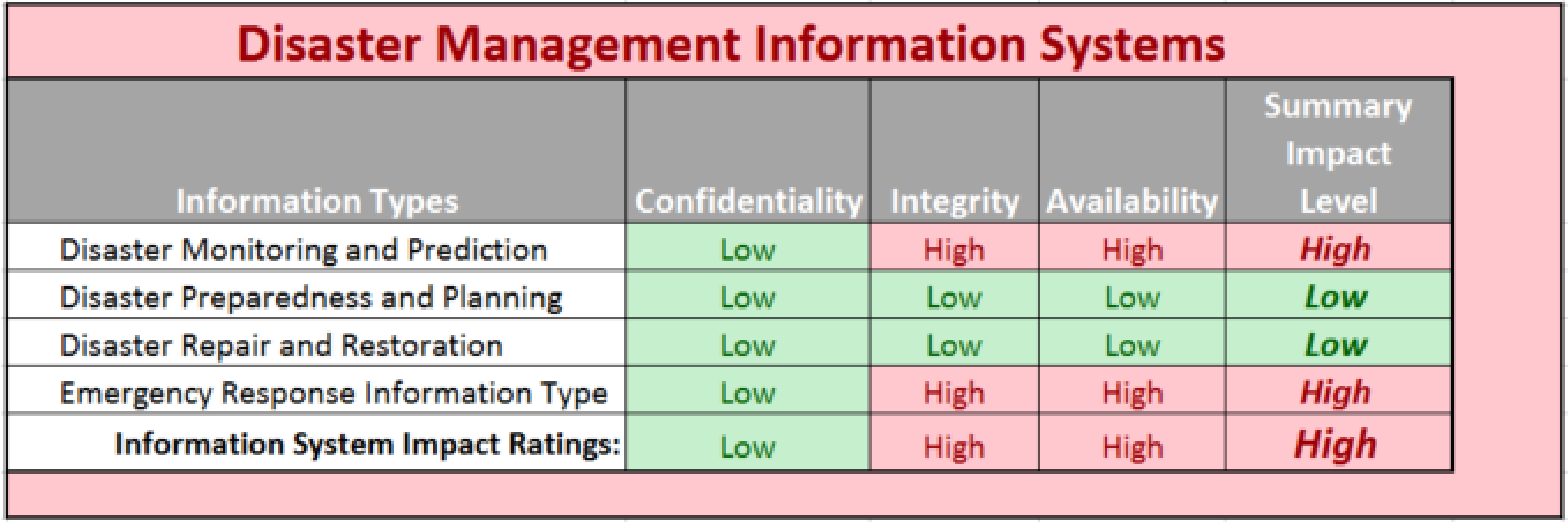


Disaster Management Information Systems

Information Types	Confidentiality	Integrity	Availability	Summary Impact Level
Disaster Monitoring and Prediction	Low	High	High	***High***
Disaster Preparedness and Planning	Low	Low	Low	***Low***
Disaster Repair and Restoration	Low	Low	Low	***Low***
Emergency Response Information Type	Low	High	High	***High***
Information System Impact Ratings:	Low	High	High	**?**

Answer

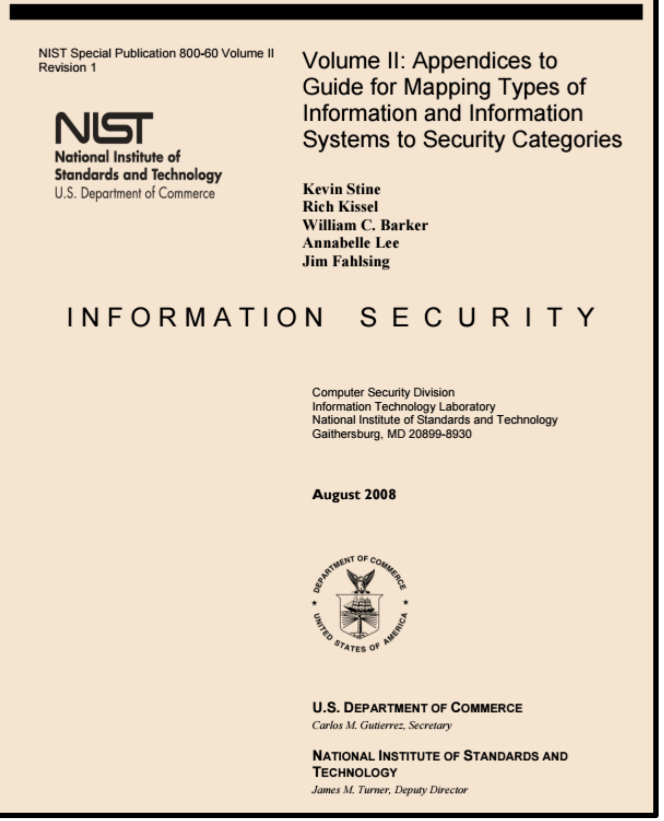
- *Overall Impact Level of Disaster Information Systems*



Disaster Management Information Systems

Information Types	Confidentiality	Integrity	Availability	Summary Impact Level
Disaster Monitoring and Prediction	Low	High	High	***High***
Disaster Preparedness and Planning	Low	Low	Low	***Low***
Disaster Repair and Restoration	Low	Low	Low	***Low***
Emergency Response Information Type	Low	High	High	***High***
Information System Impact Ratings:	Low	High	High	***High***

3. Adjust Information Impact Level



NIST Special Publication 800-60 Volume II Revision 1

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories

Kevin Stine
Rich Kissel
William C. Barker
Annabelle Lee
Jim Fahlsing

INFORMATION SECURITY

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

August 2008

U.S. DEPARTMENT OF COMMERCE
Carlos M. Gutierrez, Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
James M. Turner, Deputy Director

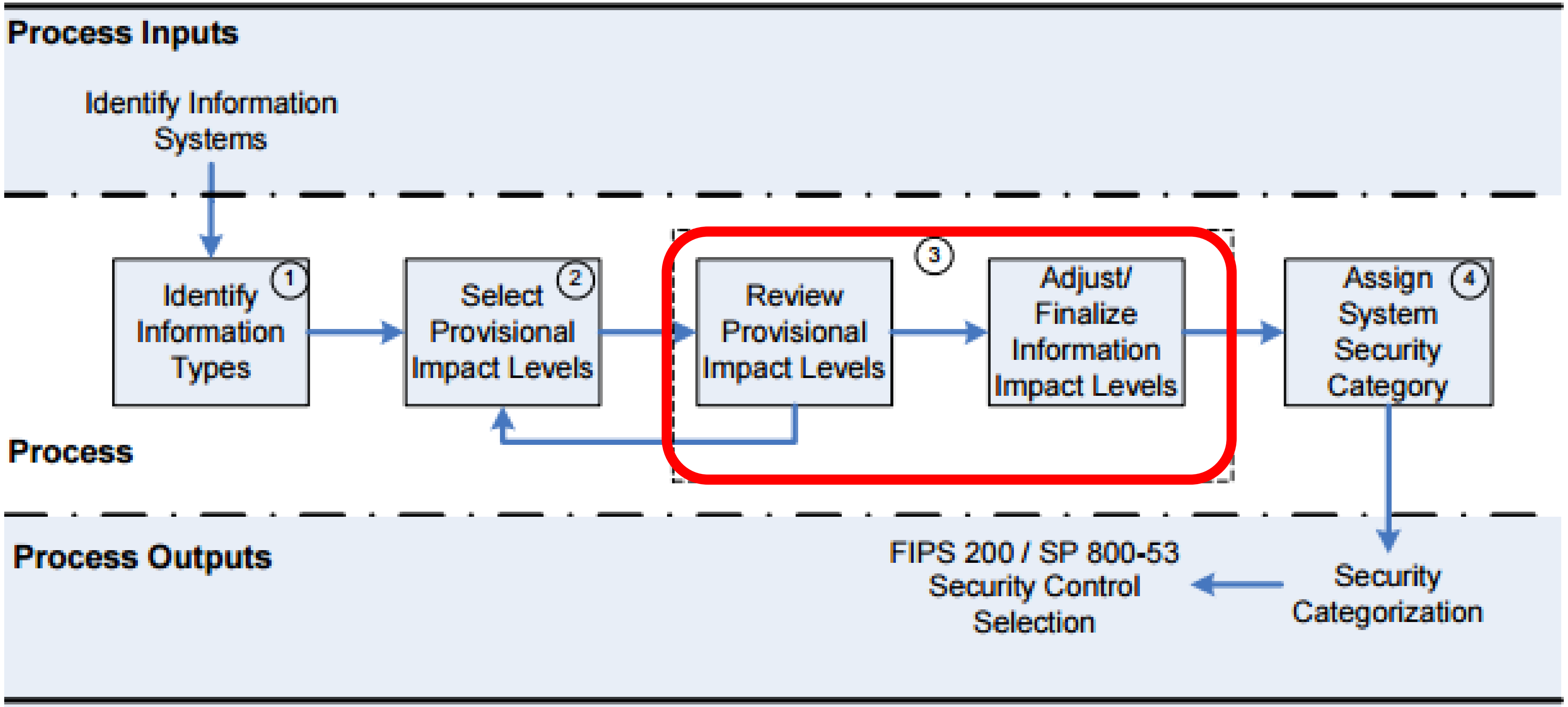
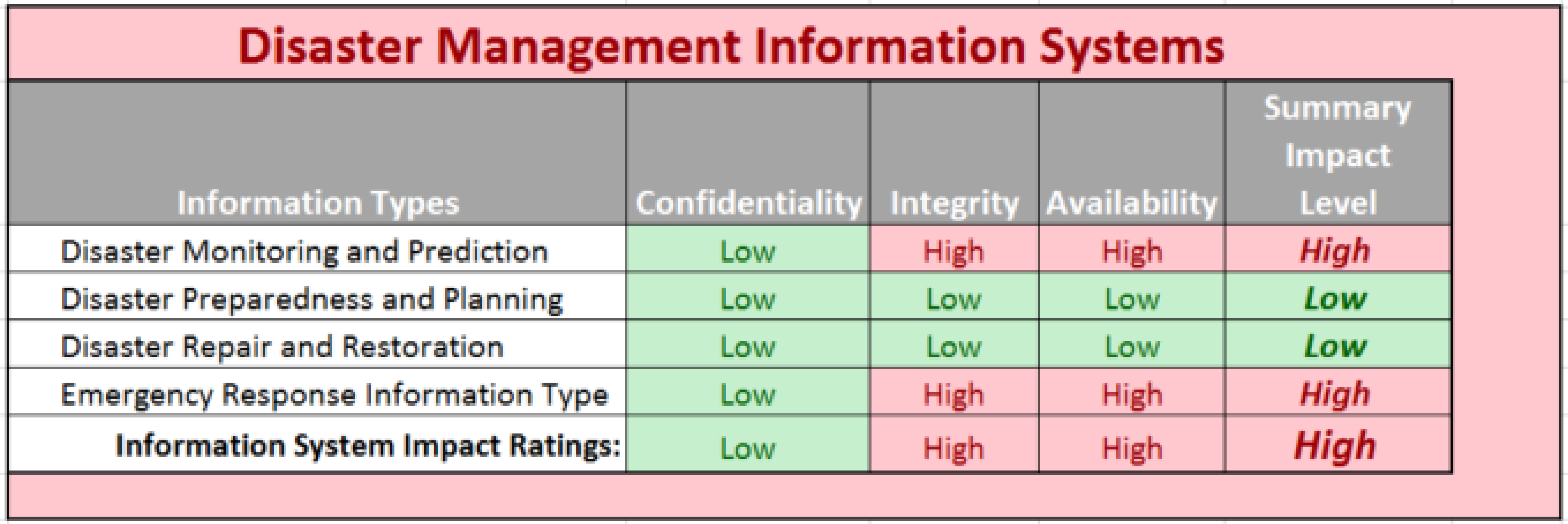

Process Inputs
Identify Information Systems
Identify Information Types
1
Select Provisional Impact Levels
2
3
Review Provisional Impact Levels
Adjust/ Finalize Information Impact Levels
Assign System Security Category
4
Process
Process Outputs
FIPS 200 / SP 800-53 Security Control Selection
Security Categorization

Figure 2: SP 800-60 Security Categorization Process Execution

To adjust preliminary impact levels…

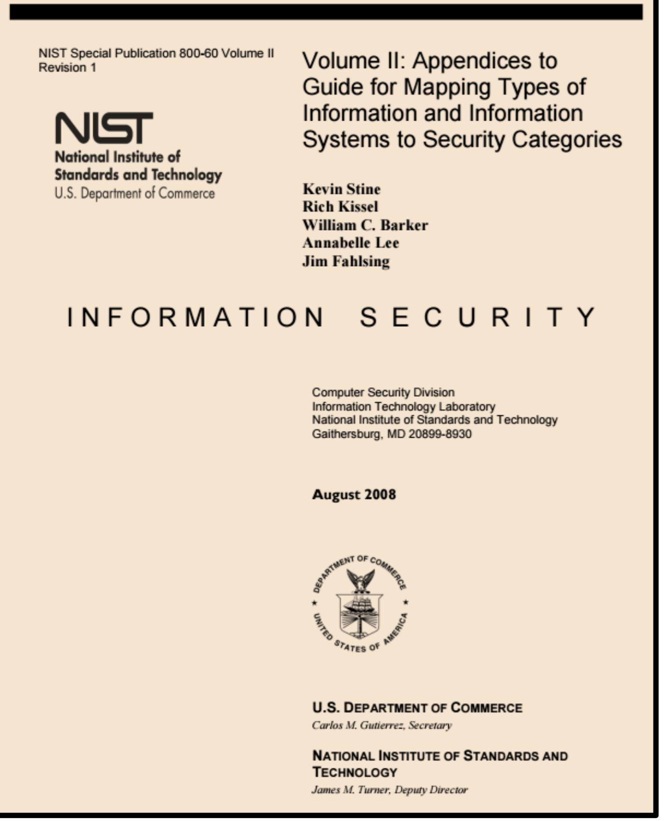
Use NIST SP 800 60 V2R1

- …looking at the "**Special Factors**" affecting CIA impact levels for each Disaster Management information type
- How might we adjust the impact levels ?



Disaster Management Information Systems

Information Types	Confidentiality	Integrity	Availability	Summary Impact Level
Disaster Monitoring and Prediction	Low	High	High	***High***
Disaster Preparedness and Planning	Low	Low	Low	***Low***
Disaster Repair and Restoration	Low	Low	Low	***Low***
Emergency Response Information Type	Low	High	High	***High***
Information System Impact Ratings:	Low	High	High	**High**



NIST Special Publication 800-60 Volume II Revision 1

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories

Kevin Stine
Rich Kissel
William C. Barker
Annabelle Lee
Jim Fahlsing

INFORMATION SECURITY

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

August 2008

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology
James M. Turner, Deputy Director

2. Select Provisional Impact Levels for the identified information system

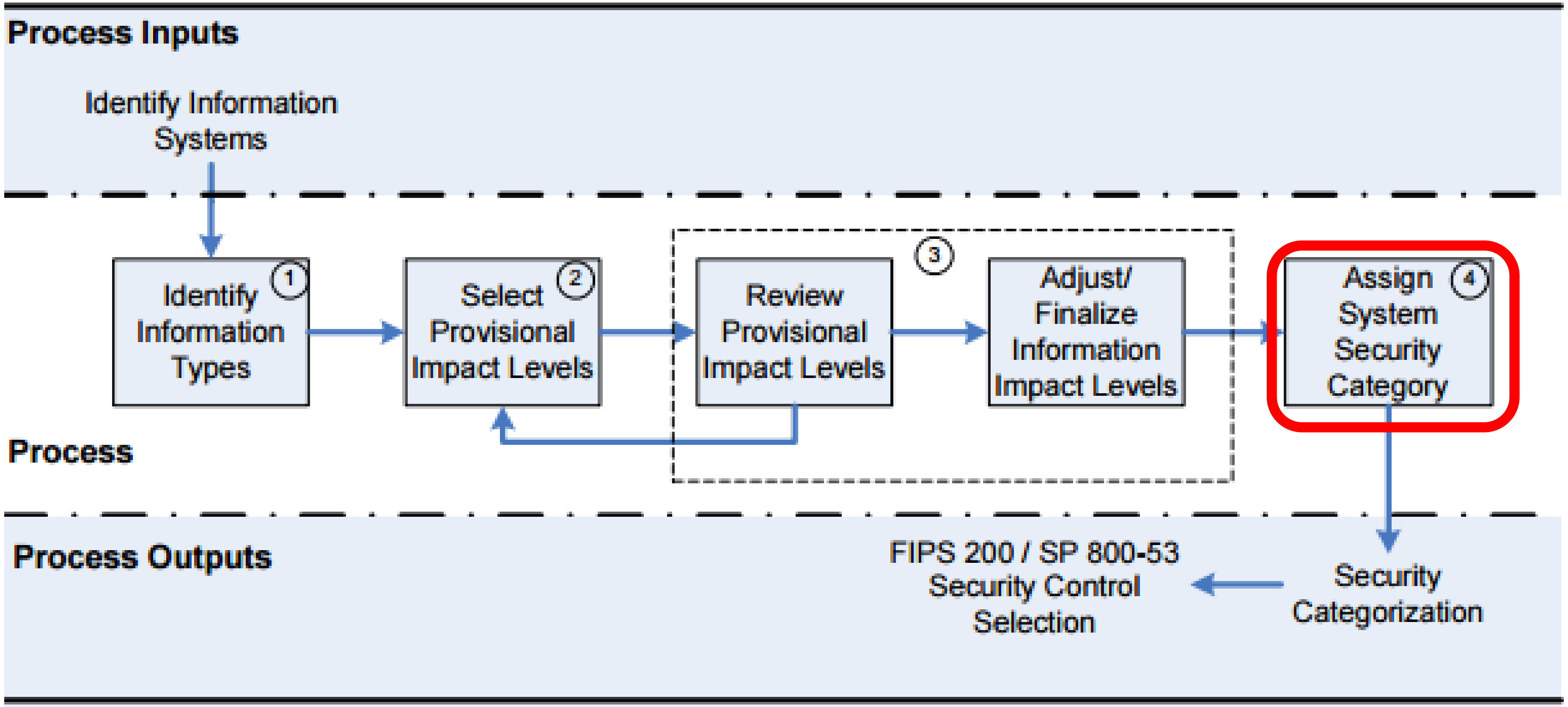
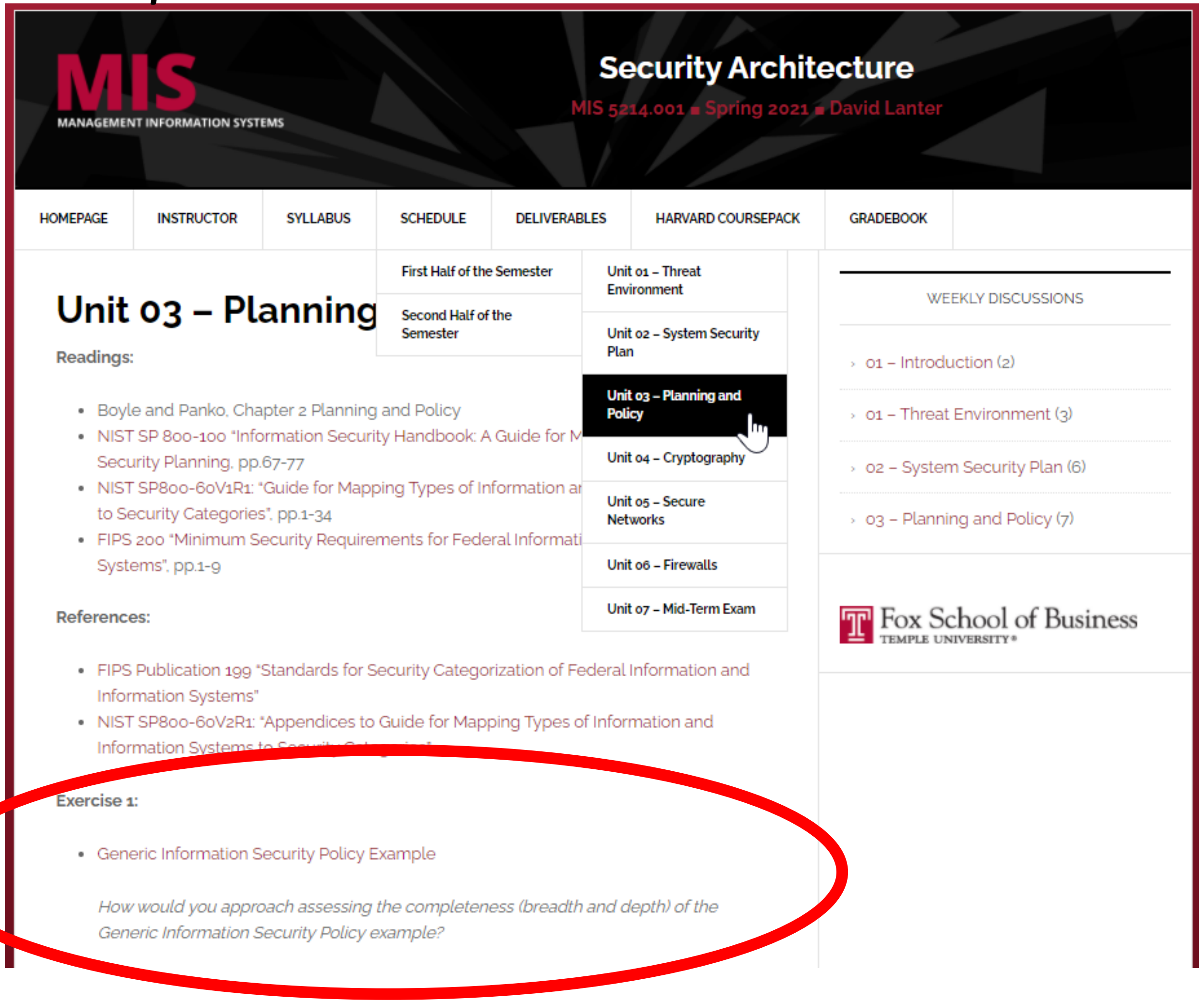

Process Inputs
Identify Information Systems
Identify Information Types 1
Select Provisional Impact Levels 2
3
Review Provisional Impact Levels
Adjust/ Finalize Information Impact Levels
Assign System Security Category 4
Process
Process Outputs
FIPS 200 / SP 800-53 Security Control Selection
Security Categorization

Figure 2: SP 800-60 Security Categorization Process Execution

Exercise: How would you approach assessing the completeness (breadth & depth) of the Generic Information Security Policy example?



MIS
MANAGEMENT INFORMATION SYSTEMS

Security Architecture
MIS 5214.001 ■ Spring 2021 ■ David Lanter

HOMEPAGE
INSTRUCTOR
SYLLABUS
SCHEDULE
DELIVERABLES
HARVARD COURSEPACK
GRADEBOOK
First Half of the Semester
Second Half of the Semester
Unit 01 – Threat Environment
Unit 02 – System Security Plan
Unit 03 – Planning and Policy
Unit 04 – Cryptography
Unit 05 – Secure Networks
Unit 06 – Firewalls
Unit 07 – Mid-Term Exam

Unit 03 – Planning

Readings:

- Boyle and Panko, Chapter 2 Planning and Policy
- NIST SP 800-100 "Information Security Handbook: A Guide for M Security Planning, pp.67-77
- NIST SP800-60V1R1: "Guide for Mapping Types of Information ar to Security Categories", pp.1-34
- FIPS 200 "Minimum Security Requirements for Federal Informati Systems", pp.1-9

References:

- FIPS Publication 199 "Standards for Security Categorization of Federal Information and Information Systems"
- NIST SP800-60V2R1: "Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories"

Exercise 1:

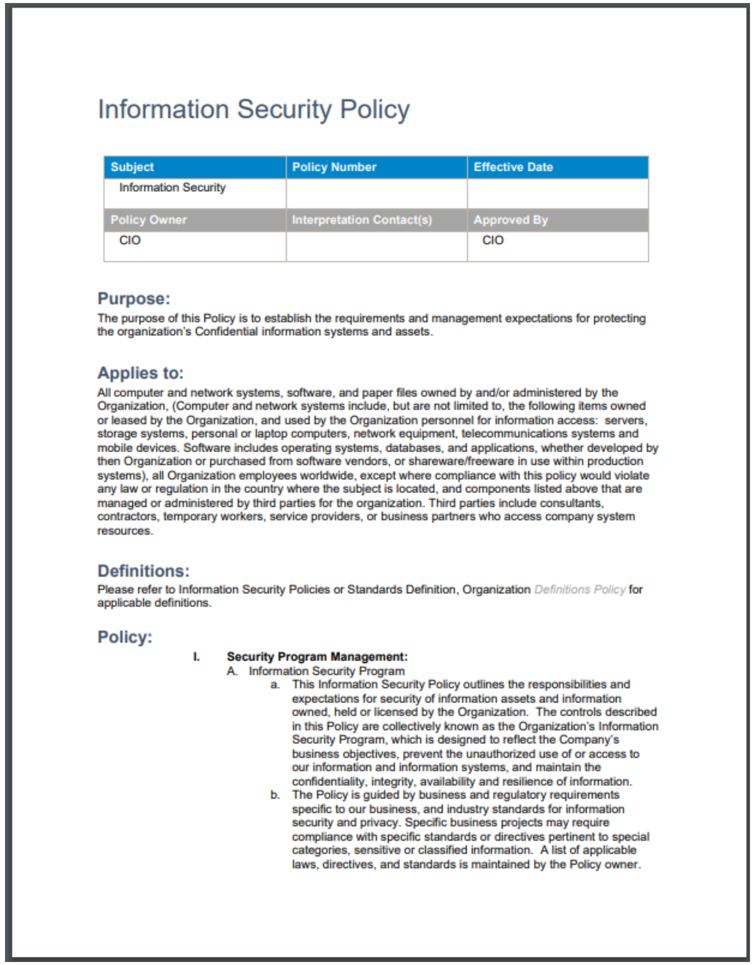
- Generic Information Security Policy Example

How would you approach assessing the completeness (breadth and depth) of the Generic Information Security Policy example?

WEEKLY DISCUSSIONS

- 01 – Introduction (2)
- 01 – Threat Environment (3)
- 02 – System Security Plan (6)
- 03 – Planning and Policy (7)

Fox School of Business
TEMPLE UNIVERSITY®



Information Security Policy

Subject	Policy Number	Effective Date
Information Security		
Policy Owner	**Interpretation Contact(s)**	**Approved By**
CIO		CIO

Purpose:

The purpose of this Policy is to establish the requirements and management expectations for protecting the organization's Confidential information systems and assets.

Applies to:

All computer and network systems, software, and paper files owned by and/or administered by the Organization, (Computer and network systems include, but are not limited to, the following items owned or leased by the Organization, and used by the Organization personnel for information access: servers, storage systems, personal or laptop computers, network equipment, telecommunications systems and mobile devices. Software includes operating systems, databases, and applications, whether developed by then Organization or purchased from software vendors, or shareware/freeware in use within production systems), all Organization employees worldwide, except where compliance with this policy would violate any law or regulation in the country where the subject is located, and components listed above that are managed or administered by third parties for the organization. Third parties include consultants, contractors, temporary workers, service providers, or business partners who access company system resources.

Definitions:

Please refer to Information Security Policies or Standards Definition, Organization *Definitions Policy* for applicable definitions.

Policy:

I. **Security Program Management:**

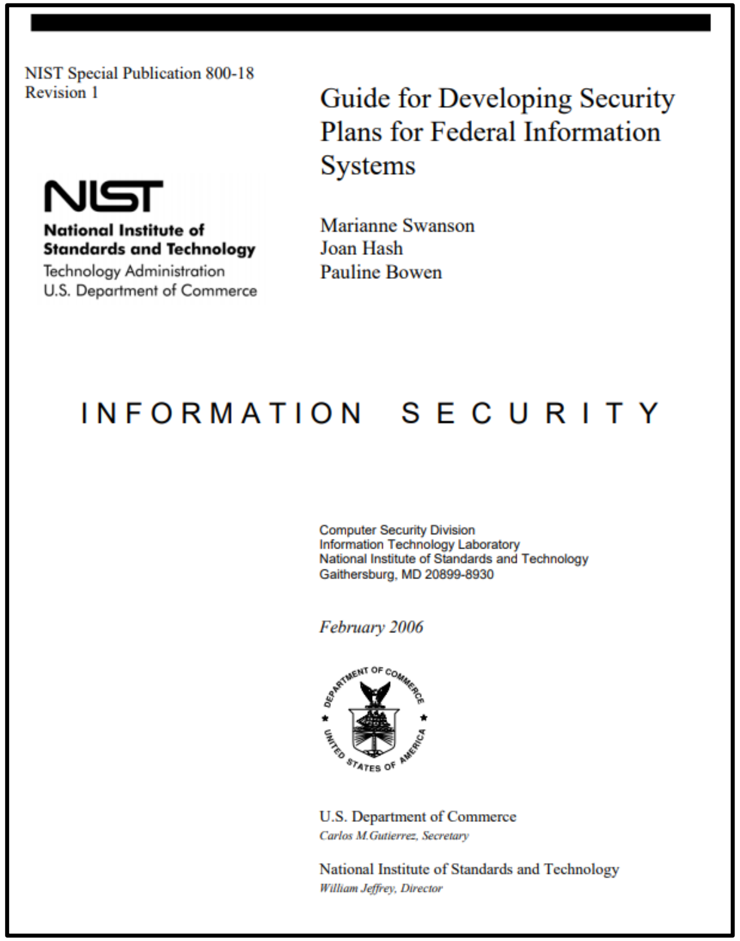
A. Information Security Program

a. This Information Security Policy outlines the responsibilities and expectations for security of information assets and information owned, held or licensed by the Organization. The controls described in this Policy are collectively known as the Organization's Information Security Program, which is designed to reflect the Company's business objectives, prevent the unauthorized use of or access to our information and information systems, and maintain the confidentiality, integrity, availability and resilience of information.

b. The Policy is guided by business and regulatory requirements specific to our business, and industry standards for information security and privacy. Specific business projects may require compliance with specific standards or directives pertinent to special categories, sensitive or classified information. A list of applicable laws, directives, and standards is maintained by the Policy owner.

Teams in Breakout Rooms

Information Security Control Families of NIST SP 800-53/800-53A grouped within 3 classes of NIST SP 800-18 provide a good framework for assessing completeness of Information Security Policies and controls



NIST Special Publication 800-18
Revision 1

Guide for Developing Security Plans for Federal Information Systems

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Marianne Swanson
Joan Hash
Pauline Bowen

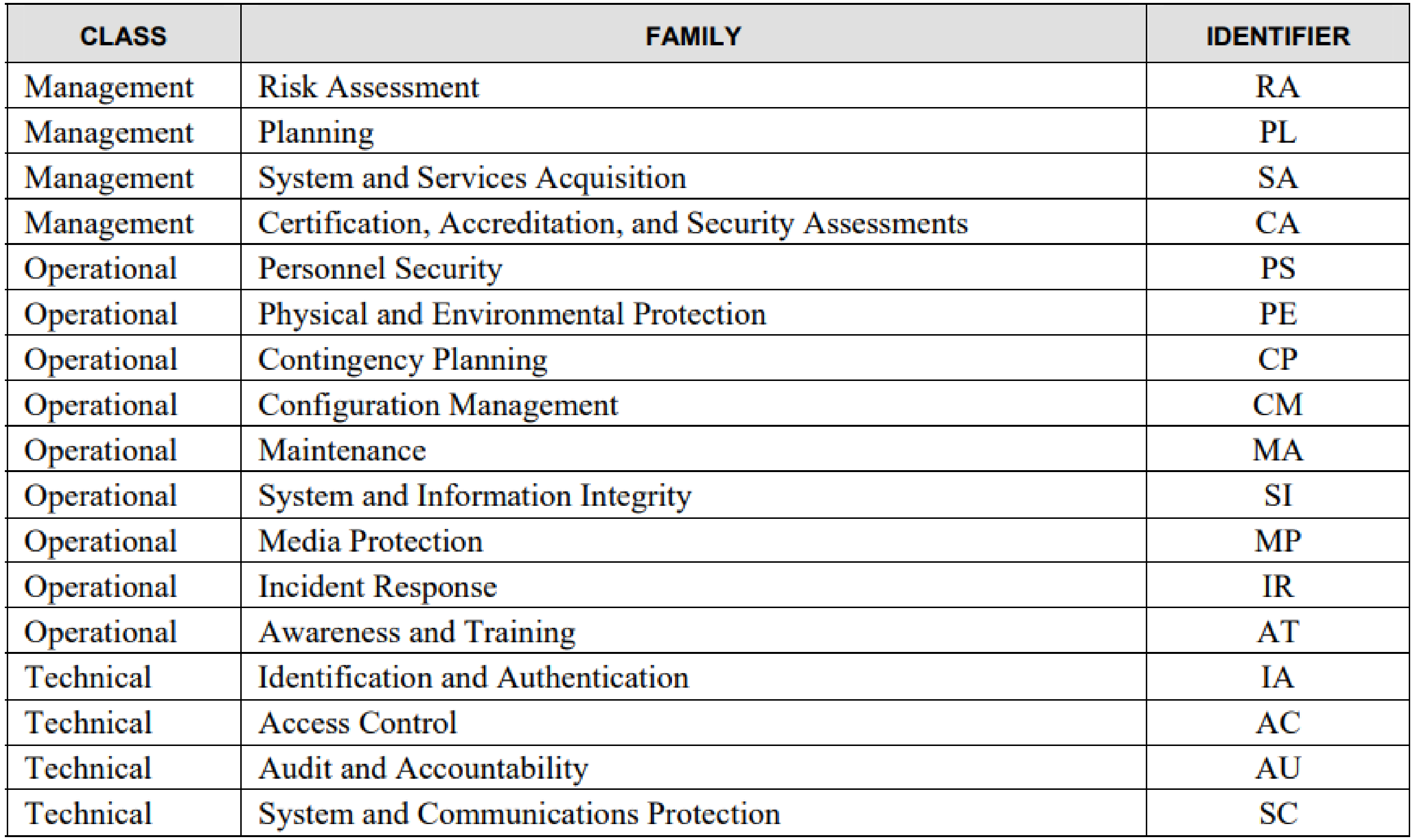
INFORMATION SECURITY

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

February 2006

U.S. Department of Commerce
Carlos M.Gutierrez, Secretary

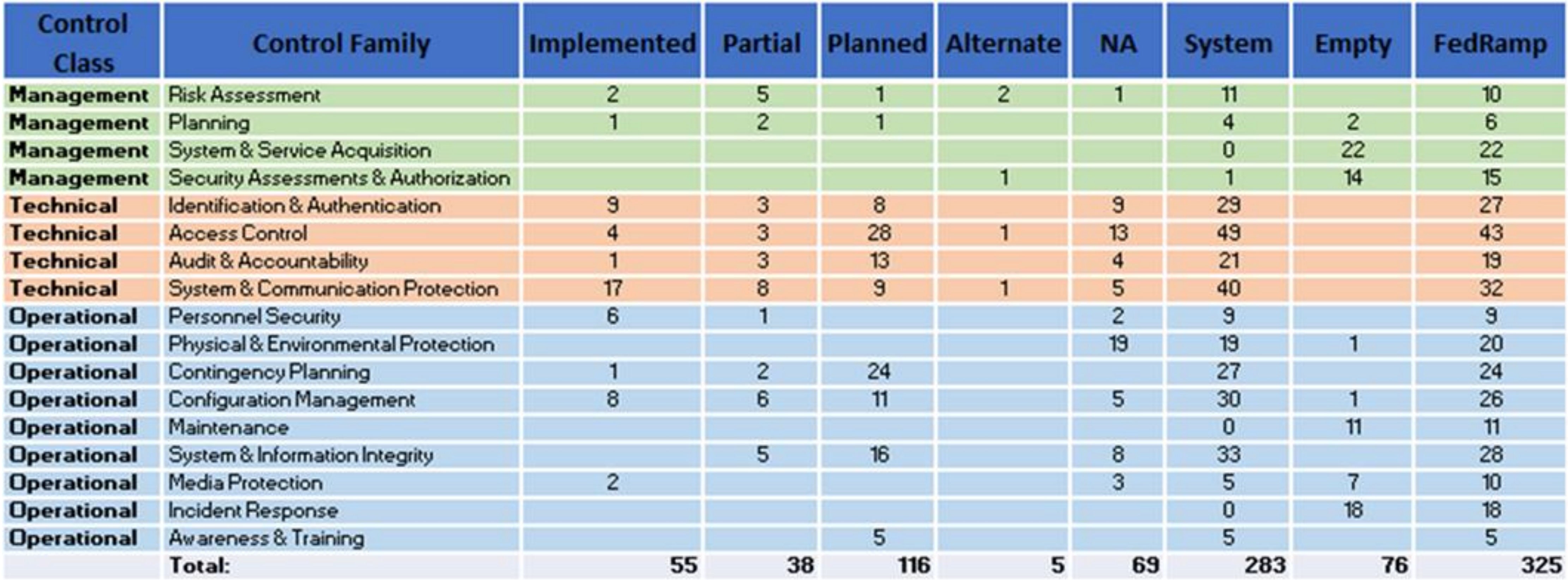
National Institute of Standards and Technology
William Jeffrey, Director



CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and Security Assessments	CA
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency Planning	CP
Operational	Configuration Management	CM
Operational	Maintenance	MA
Operational	System and Information Integrity	SI
Operational	Media Protection	MP
Operational	Incident Response	IR
Operational	Awareness and Training	AT
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

Table 2: Security Control Class, Family, and Identifier

Information Security Control Families of NIST SP 800-53/800-53A grouped within 3 Control Classes of NIST SP 800-18 provide a framework for assessing completeness of Information Security Policies and controls



Control Class	Control Family	Implemented	Partial	Planned	Alternate	NA	System	Empty	FedRamp
Management	Risk Assessment	2	5	1	2	1	11		10
Management	Planning	1	2	1			4	2	6
Management	System & Service Acquisition						0	22	22
Management	Security Assessments & Authorization				1		1	14	15
Technical	Identification & Authentication	9	3	8		9	29		27
Technical	Access Control	4	3	28	1	13	49		43
Technical	Audit & Accountability	1	3	13		4	21		19
Technical	System & Communication Protection	17	8	9	1	5	40		32
Operational	Personnel Security	6	1			2	9		9
Operational	Physical & Environmental Protection					19	19	1	20
Operational	Contingency Planning	1	2	24			27		24
Operational	Configuration Management	8	6	11		5	30	1	26
Operational	Maintenance						0	11	11
Operational	System & Information Integrity		5	16		8	33		28
Operational	Media Protection	2				3	5	7	10
Operational	Incident Response						0	18	18
Operational	Awareness & Training			5			5		5
	Total:	55	38	116	5	69	283	76	325

Completeness?

Exercise

Using NIST SP 800-60, find a preliminary categorization for the following information system and adjust the categorization based on your analysis – present justifications for both preliminary and adjusted categorizations

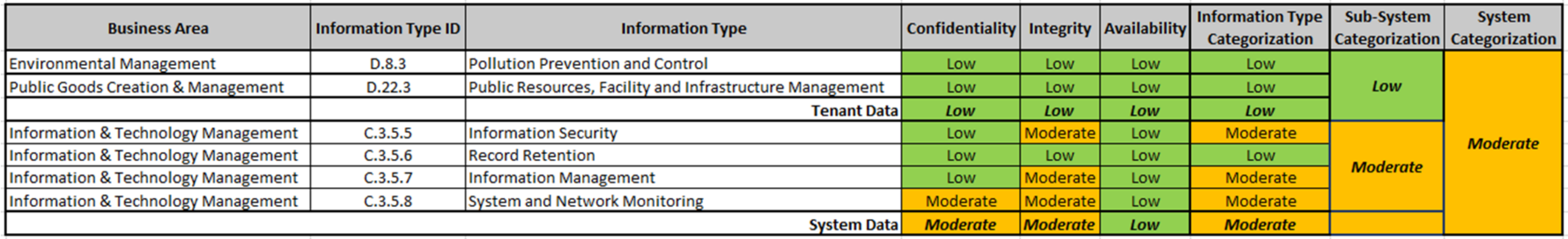
Purpose: The system has two overarching purposes:

1. For clients it is a system intended to help understand sewage and storm water collection and treatment systems (i.e. pipe networks, pump stations, and treatment plants) and their capacities, overflow characteristics and controls
2. For the firm the system is intended to provide revenue through pay by clients for direct use of the service(s) of the system

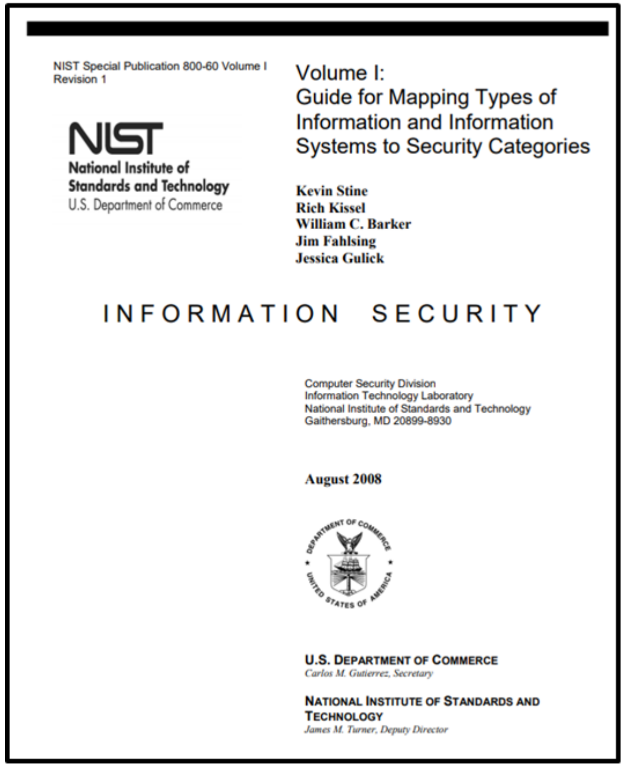
Users:

1. Municipal and regional water and sewer utilities and governmental organizations will use the system to help plan capital improvement, operations, and maintenance of sewer systems (i.e. treatment plants and sewage collection networks)
2. External consultants helping municipal and regional water and sewer utilities plan capital improvement, operations, and maintenance of sewer systems
3. The firm's technical information system development staff will work directly on the information system to provide, maintain, enhance and extend the services of the information system

Below is a preliminary categorization for the information system based on NIST SP 800-60 Vol



Business Area	Information Type ID	Information Type	Confidentiality	Integrity	Availability	Information Type Categorization	Sub-System Categorization	System Categorization
Environmental Management	D.8.3	Pollution Prevention and Control	Low	Low	Low	Low	*Low*	*Moderate*
Public Goods Creation & Management	D.22.3	Public Resources, Facility and Infrastructure Management	Low	Low	Low	Low		
		Tenant Data	***Low***	***Low***	***Low***	***Low***		
Information & Technology Management	C.3.5.5	Information Security	Low	Moderate	Low	Moderate	*Moderate*	
Information & Technology Management	C.3.5.6	Record Retention	Low	Low	Low	Low		
Information & Technology Management	C.3.5.7	Information Management	Low	Moderate	Low	Moderate		
Information & Technology Management	C.3.5.8	System and Network Monitoring	Moderate	Moderate	Low	Moderate		
		System Data	***Moderate***	***Moderate***	***Low***	***Moderate***		



NIST Special Publication 800-60 Volume I
Revision 1

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Volume I:
Guide for Mapping Types of Information and Information Systems to Security Categories

Kevin Stine
Rich Kissel
William C. Barker
Jim Fahlsing
Jessica Gulick

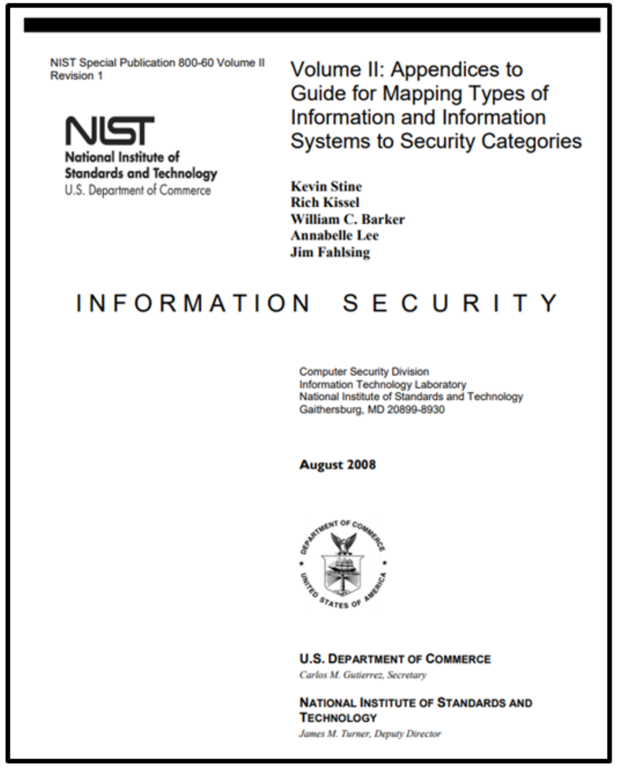
INFORMATION SECURITY

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

August 2008

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology
James M. Turner, Deputy Director



NIST Special Publication 800-60 Volume II
Revision 1

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Volume II: Appendices to
Guide for Mapping Types of Information and Information Systems to Security Categories

Kevin Stine
Rich Kissel
William C. Barker
Annabelle Lee
Jim Fahlsing

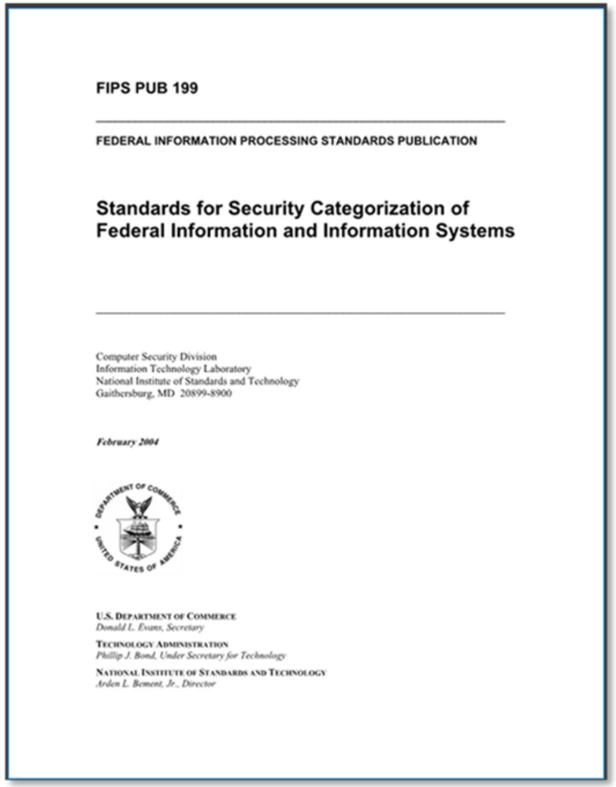
INFORMATION SECURITY

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

August 2008

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology
James M. Turner, Deputy Director



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

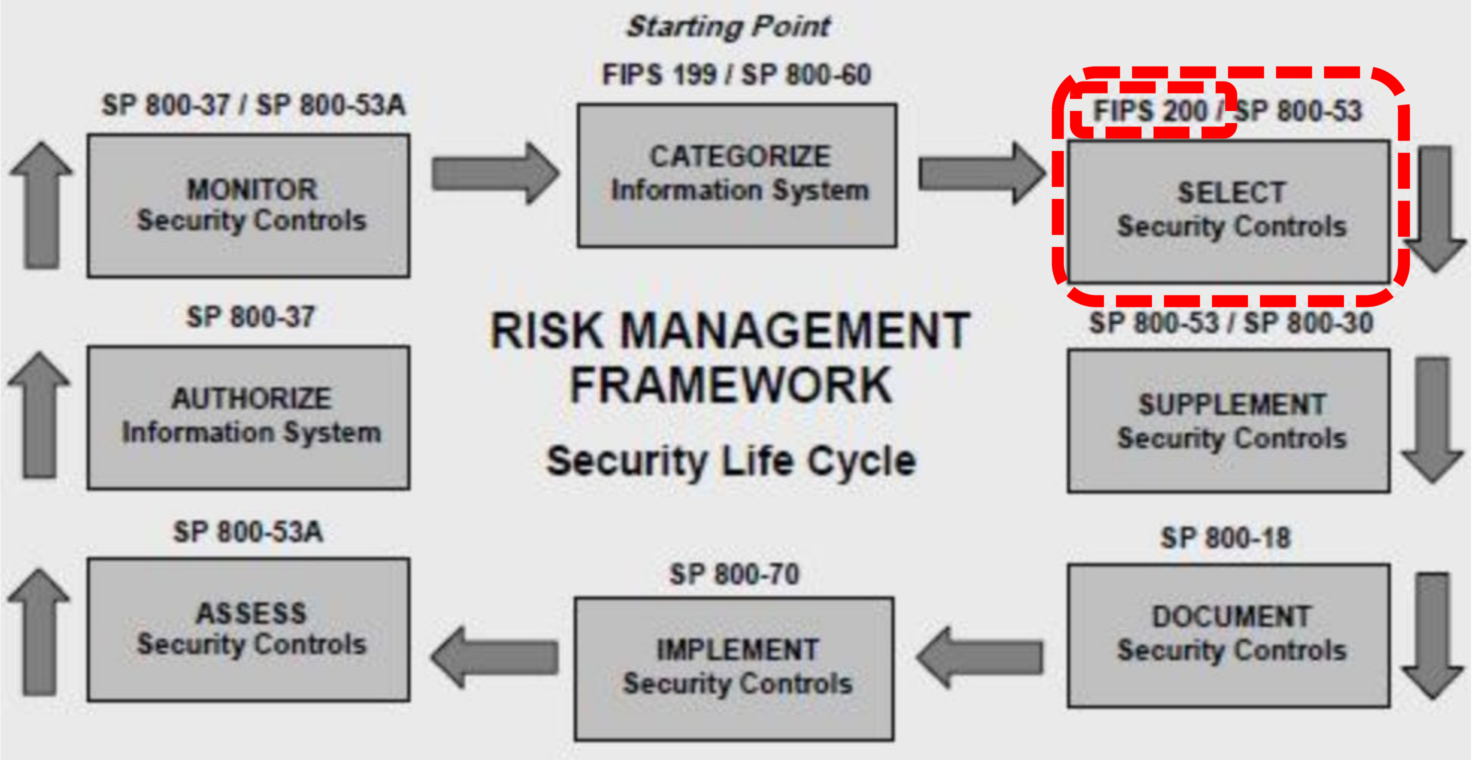
Technology Administration
Phillip J. Bond, Under Secretary for Technology

National Institute of Standards and Technology
Arden L. Bement, Jr., Director

Agenda

- ✓Risk Management Framework and IS Security Categorization
- ✓Mapping Information Types to Security Categorizations
- ✓*Exercises – Determine and finalize impact levels*
- ✓*Exercise – Determine Information and Information System Types and provisional security categorization*
- Security Control Baselines – review
  - Minimum Security Controls and Security Control Baselines
  - Security Control Families
- Risk Assessment Controls
- Team Exercise *Find and assess risk assessment policy*

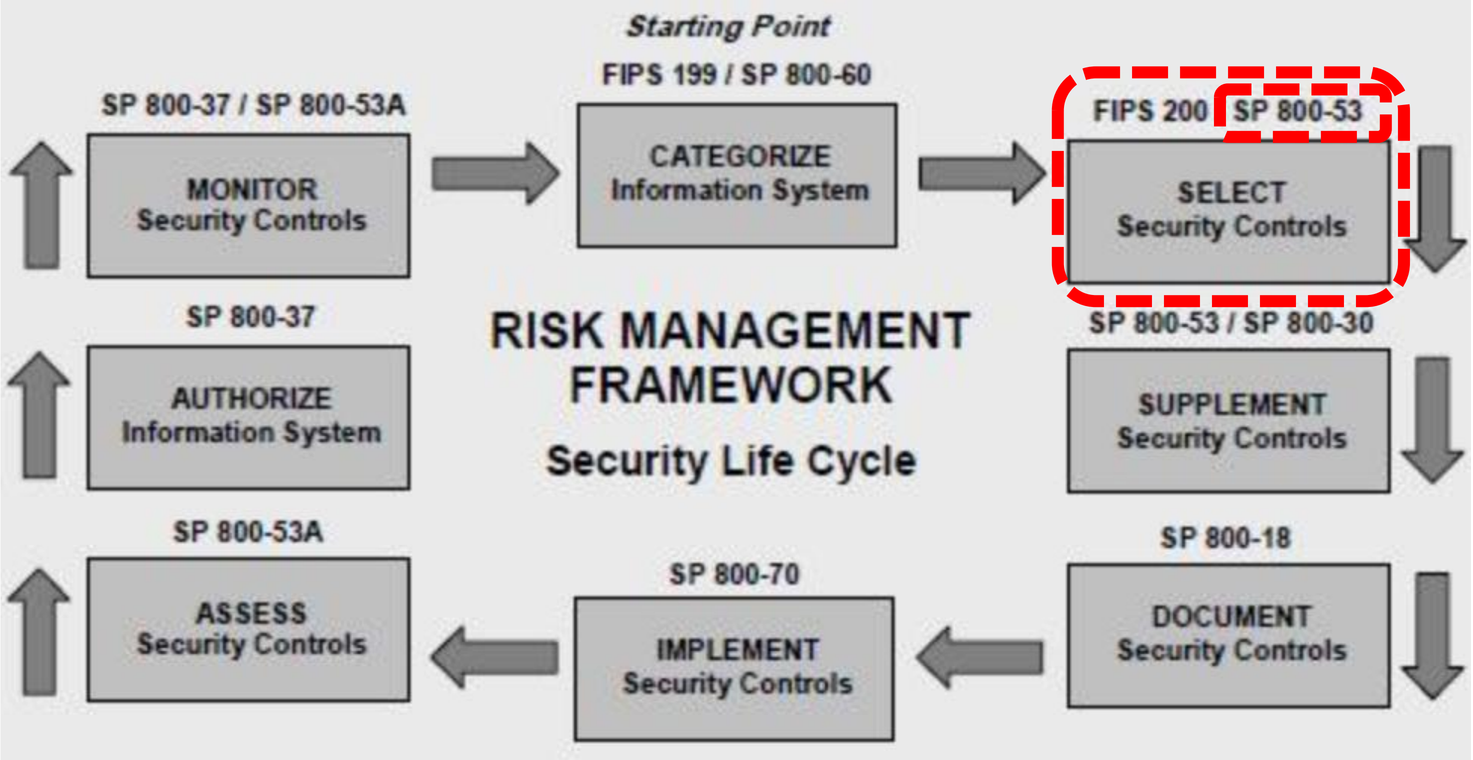
Risk Management Framework

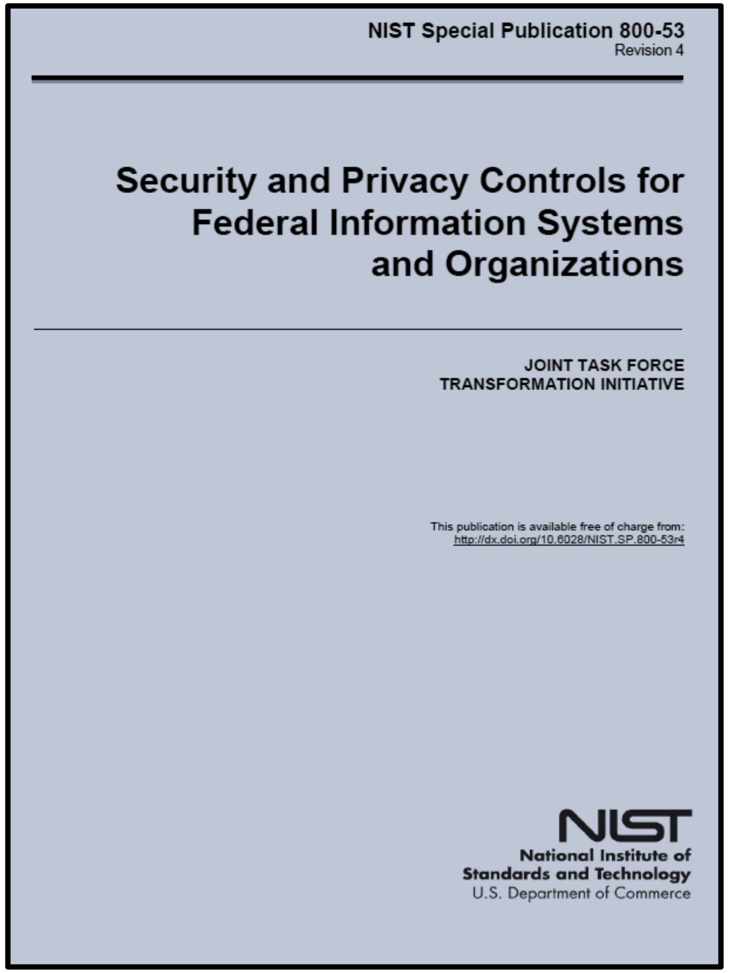


Minimum Security Control Requirements

1. Access Control (AC)
2. Awareness and Training (AT)
3. Audit and Accountability (AU)
4. Certification, Accreditation, and Security Assessment (CA)
5. Configuration Management (CM)
6. Contingency Planning
7. Identification and Authentication
8. Incident Response (IR)
9. Maintenance (MA)
10. Media Protection (MP)
11. Physical and Environmental Protection *PE)
12. Planning (PL)
13. Personal Security (PS)
14. Risk Assessment (RA)
15. System and Services Acquisition(SA)
16. System and Communications Protection (SC)
17. System and Information Integrity (SI)

Risk Management Framework





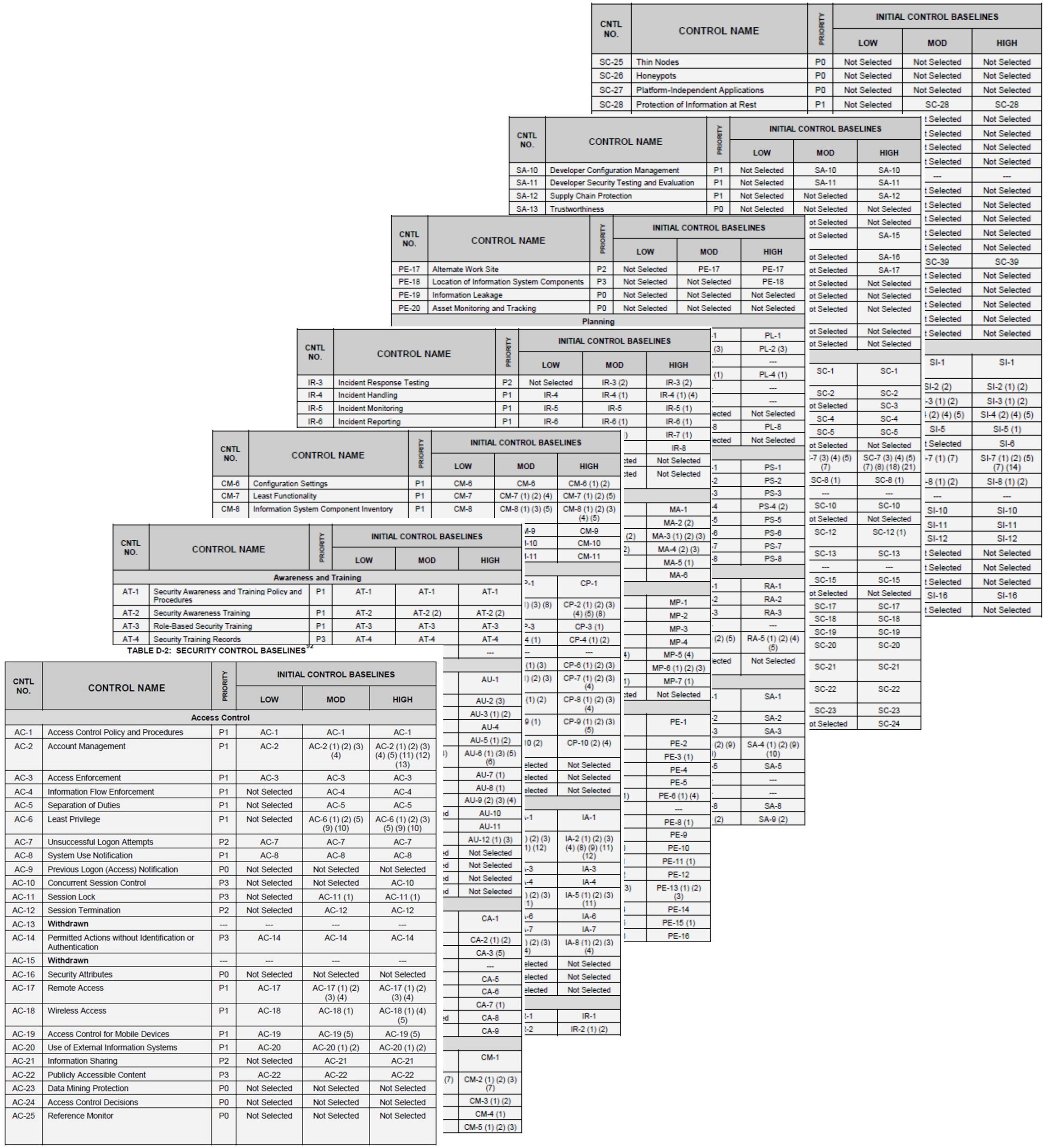
NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-53r4

National Institute of Standards and Technology
U.S. Department of Commerce



CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
SC-25	Thin Nodes	P0	Not Selected	Not Selected	Not Selected
SC-26	Honeypots	P0	Not Selected	Not Selected	Not Selected
SC-27	Platform-Independent Applications	P0	Not Selected	Not Selected	Not Selected
SC-28	Protection of Information at Rest	P1	Not Selected	SC-28	SC-28

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
SA-10	Developer Configuration Management	P1	Not Selected	SA-10	SA-10
SA-11	Developer Security Testing and Evaluation	P1	Not Selected	SA-11	SA-11
SA-12	Supply Chain Protection	P1	Not Selected	Not Selected	SA-12
SA-13	Trustworthiness	P0	Not Selected	Not Selected	Not Selected

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
PE-17	Alternate Work Site	P2	Not Selected	PE-17	PE-17
PE-18	Location of Information System Components	P3	Not Selected	Not Selected	PE-18
PE-19	Information Leakage	P0	Not Selected	Not Selected	Not Selected
PE-20	Asset Monitoring and Tracking	P0	Not Selected	Not Selected	Not Selected
Planning					

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
IR-3	Incident Response Testing	P2	Not Selected	IR-3 (2)	IR-3 (2)
IR-4	Incident Handling	P1	IR-4	IR-4 (1)	IR-4 (1) (4)
IR-5	Incident Monitoring	P1	IR-5	IR-5	IR-5 (1)
IR-6	Incident Reporting	P1	IR-6	IR-6 (1)	IR-6 (1)

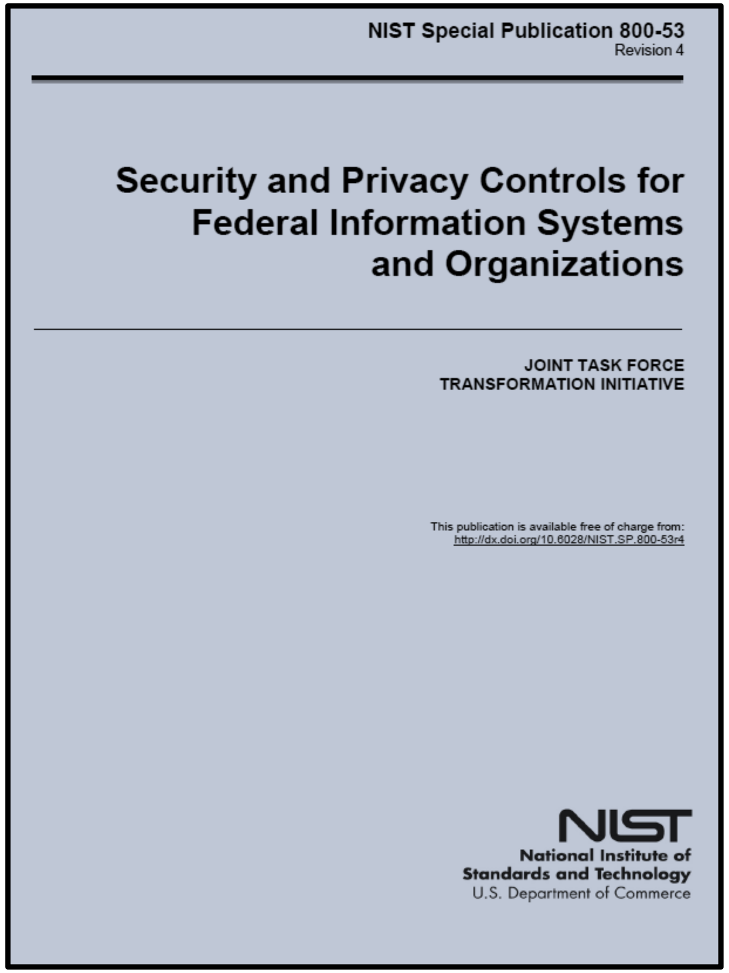
CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
CM-6	Configuration Settings	P1	CM-6	CM-6	CM-6 (1) (2)
CM-7	Least Functionality	P1	CM-7	CM-7 (1) (2) (4)	CM-7 (1) (2) (5)
CM-8	Information System Component Inventory	P1	CM-8	CM-8 (1) (3) (5)	CM-8 (1) (2) (3) (4) (5)

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Awareness and Training					
AT-1	Security Awareness and Training Policy and Procedures	P1	AT-1	AT-1	AT-1
AT-2	Security Awareness Training	P1	AT-2	AT-2 (2)	AT-2 (2)
AT-3	Role-Based Security Training	P1	AT-3	AT-3	AT-3
AT-4	Security Training Records	P3	AT-4	AT-4	AT-4

TABLE D-2: SECURITY CONTROL BASELINES[92]

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Access Control					
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5
AC-6	Least Privilege	P1	Not Selected	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)
AC-7	Unsuccessful Logon Attempts	P2	AC-7	AC-7	AC-7
AC-8	System Use Notification	P1	AC-8	AC-8	AC-8
AC-9	Previous Logon (Access) Notification	P0	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	P3	Not Selected	Not Selected	AC-10
AC-11	Session Lock	P3	Not Selected	AC-11 (1)	AC-11 (1)
AC-12	Session Termination	P2	Not Selected	AC-12	AC-12
AC-13	**Withdrawn**	---	---	---	---
AC-14	Permitted Actions without Identification or Authentication	P3	AC-14	AC-14	AC-14
AC-15	**Withdrawn**	---	---	---	---
AC-16	Security Attributes	P0	Not Selected	Not Selected	Not Selected
AC-17	Remote Access	P1	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)
AC-18	Wireless Access	P1	AC-18	AC-18 (1)	AC-18 (1) (4) (5)
AC-19	Access Control for Mobile Devices	P1	AC-19	AC-19 (5)	AC-19 (5)
AC-20	Use of External Information Systems	P1	AC-20	AC-20 (1) (2)	AC-20 (1) (2)
AC-21	Information Sharing	P2	Not Selected	AC-21	AC-21
AC-22	Publicly Accessible Content	P3	AC-22	AC-22	AC-22
AC-23	Data Mining Protection	P0	Not Selected	Not Selected	Not Selected
AC-24	Access Control Decisions	P0	Not Selected	Not Selected	Not Selected
AC-25	Reference Monitor	P0	Not Selected	Not Selected	Not Selected

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf



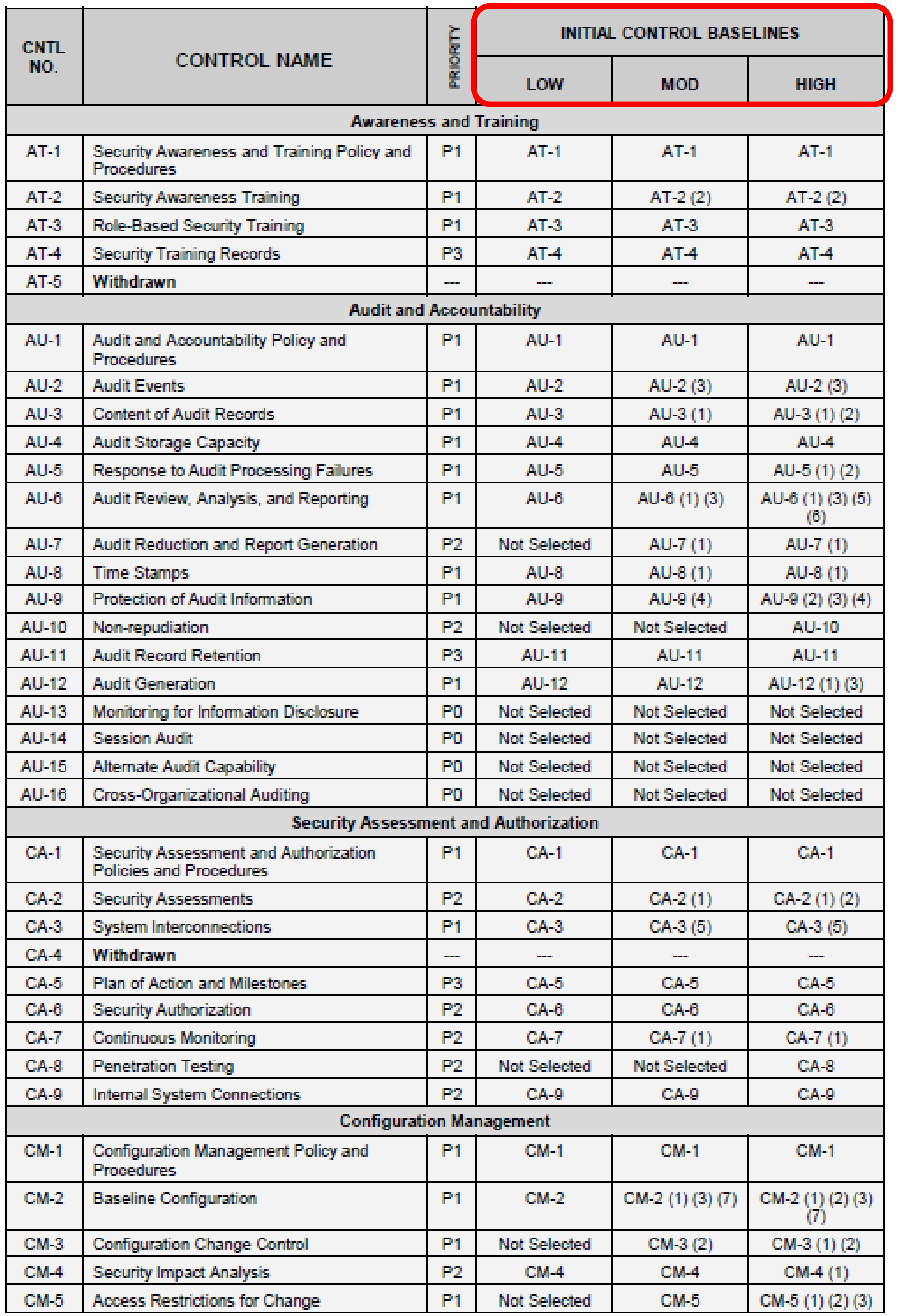
NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

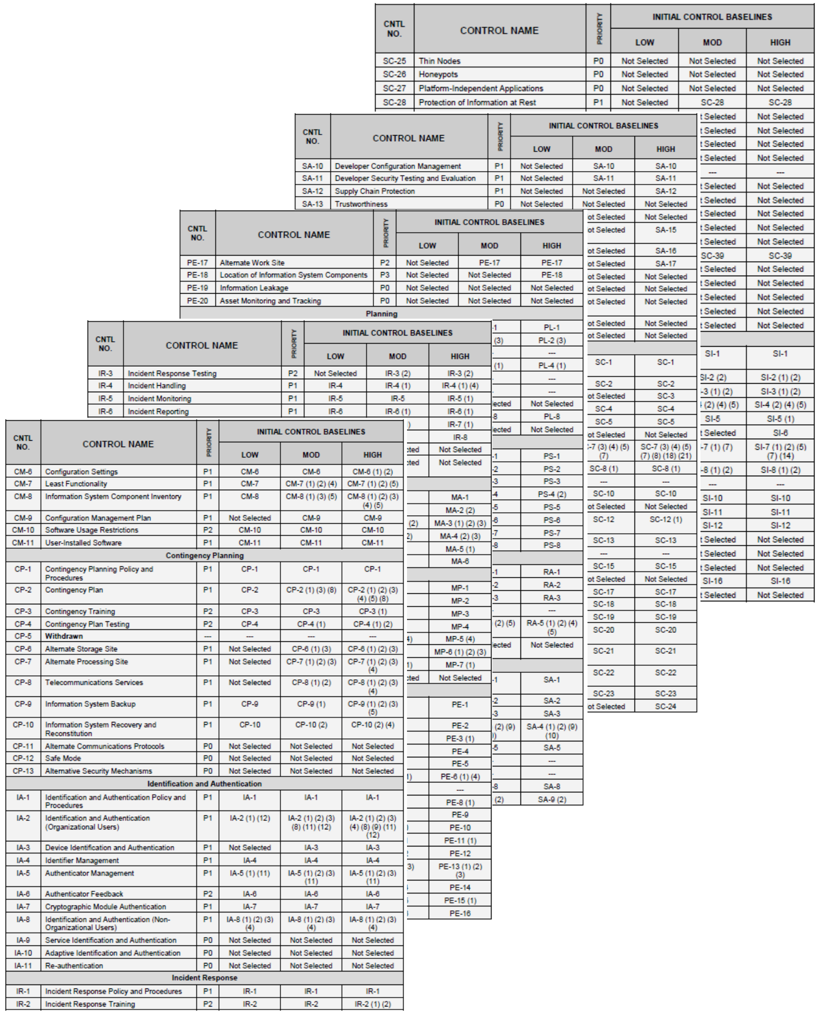
JOINT TASK FORCE
TRANSFORMATION INITIATIVE

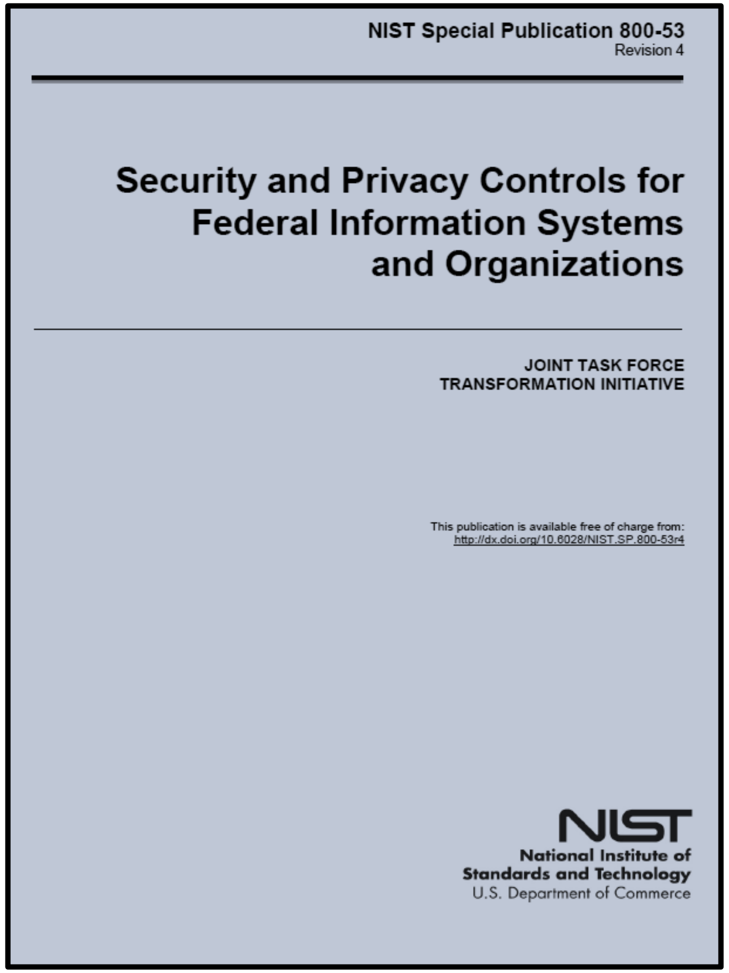
This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-53r4

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce



CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
	Awareness and Training				
AT-1	Security Awareness and Training Policy and Procedures	P1	AT-1	AT-1	AT-1
AT-2	Security Awareness Training	P1	AT-2	AT-2 (2)	AT-2 (2)
AT-3	Role-Based Security Training	P1	AT-3	AT-3	AT-3
AT-4	Security Training Records	P3	AT-4	AT-4	AT-4
AT-5	**Withdrawn**	---	---	---	---
	Audit and Accountability				
AU-1	Audit and Accountability Policy and Procedures	P1	AU-1	AU-1	AU-1
AU-2	Audit Events	P1	AU-2	AU-2 (3)	AU-2 (3)
AU-3	Content of Audit Records	P1	AU-3	AU-3 (1)	AU-3 (1) (2)
AU-4	Audit Storage Capacity	P1	AU-4	AU-4	AU-4
AU-5	Response to Audit Processing Failures	P1	AU-5	AU-5	AU-5 (1) (2)
AU-6	Audit Review, Analysis, and Reporting	P1	AU-6	AU-6 (1) (3)	AU-6 (1) (3) (5) (6)
AU-7	Audit Reduction and Report Generation	P2	Not Selected	AU-7 (1)	AU-7 (1)
AU-8	Time Stamps	P1	AU-8	AU-8 (1)	AU-8 (1)
AU-9	Protection of Audit Information	P1	AU-9	AU-9 (4)	AU-9 (2) (3) (4)
AU-10	Non-repudiation	P2	Not Selected	Not Selected	AU-10
AU-11	Audit Record Retention	P3	AU-11	AU-11	AU-11
AU-12	Audit Generation	P1	AU-12	AU-12	AU-12 (1) (3)
AU-13	Monitoring for Information Disclosure	P0	Not Selected	Not Selected	Not Selected
AU-14	Session Audit	P0	Not Selected	Not Selected	Not Selected
AU-15	Alternate Audit Capability	P0	Not Selected	Not Selected	Not Selected
AU-16	Cross-Organizational Auditing	P0	Not Selected	Not Selected	Not Selected
	Security Assessment and Authorization				
CA-1	Security Assessment and Authorization Policies and Procedures	P1	CA-1	CA-1	CA-1
CA-2	Security Assessments	P2	CA-2	CA-2 (1)	CA-2 (1) (2)
CA-3	System Interconnections	P1	CA-3	CA-3 (5)	CA-3 (5)
CA-4	**Withdrawn**	---	---	---	---
CA-5	Plan of Action and Milestones	P3	CA-5	CA-5	CA-5
CA-6	Security Authorization	P2	CA-6	CA-6	CA-6
CA-7	Continuous Monitoring	P2	CA-7	CA-7 (1)	CA-7 (1)
CA-8	Penetration Testing	P2	Not Selected	Not Selected	CA-8
CA-9	Internal System Connections	P2	CA-9	CA-9	CA-9
	Configuration Management				
CM-1	Configuration Management Policy and Procedures	P1	CM-1	CM-1	CM-1
CM-2	Baseline Configuration	P1	CM-2	CM-2 (1) (3) (7)	CM-2 (1) (2) (3) (7)
CM-3	Configuration Change Control	P1	Not Selected	CM-3 (2)	CM-3 (1) (2)
CM-4	Security Impact Analysis	P2	CM-4	CM-4	CM-4 (1)
CM-5	Access Restrictions for Change	P1	Not Selected	CM-5	CM-5 (1) (2) (3)





NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-53r4

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

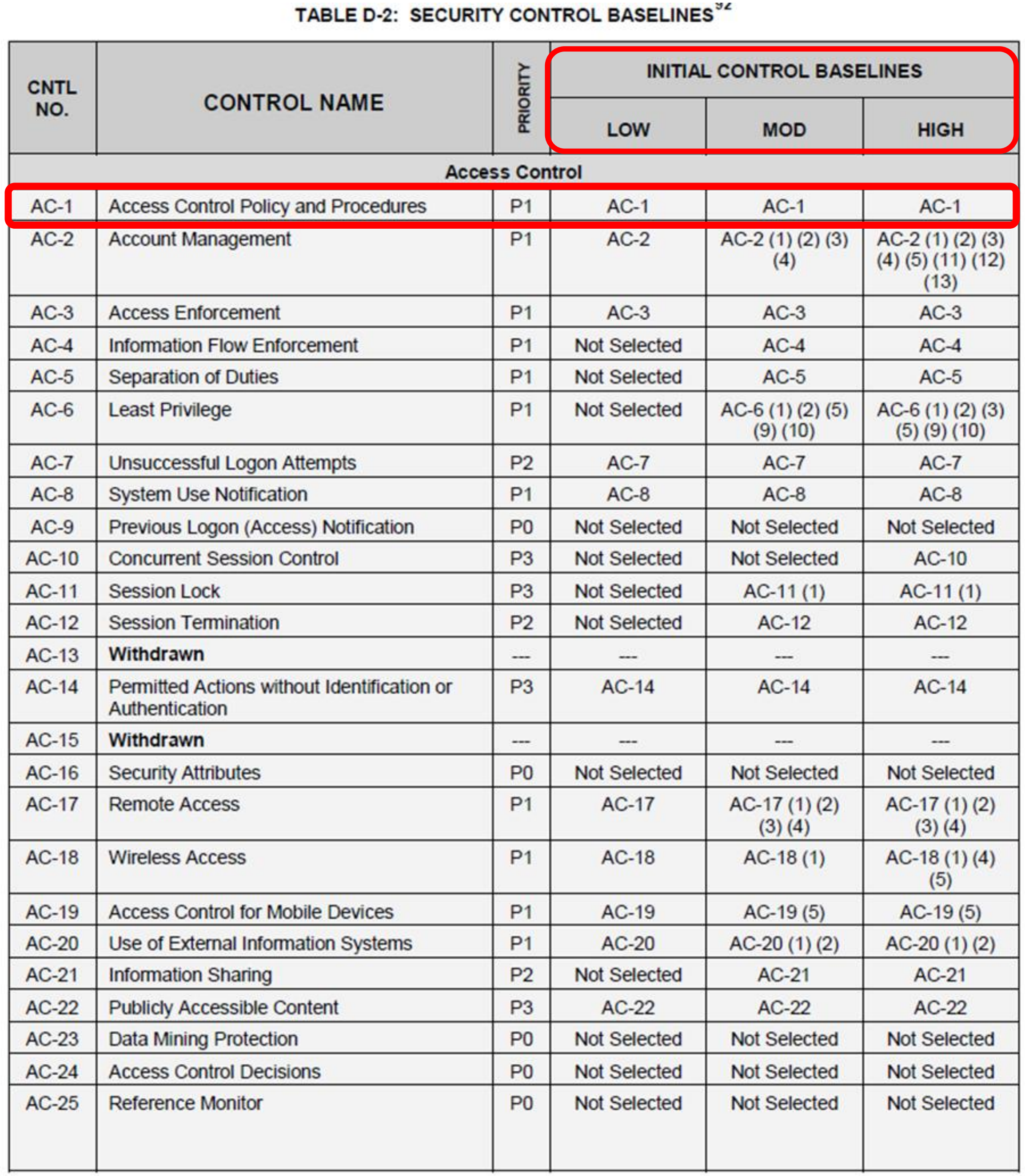
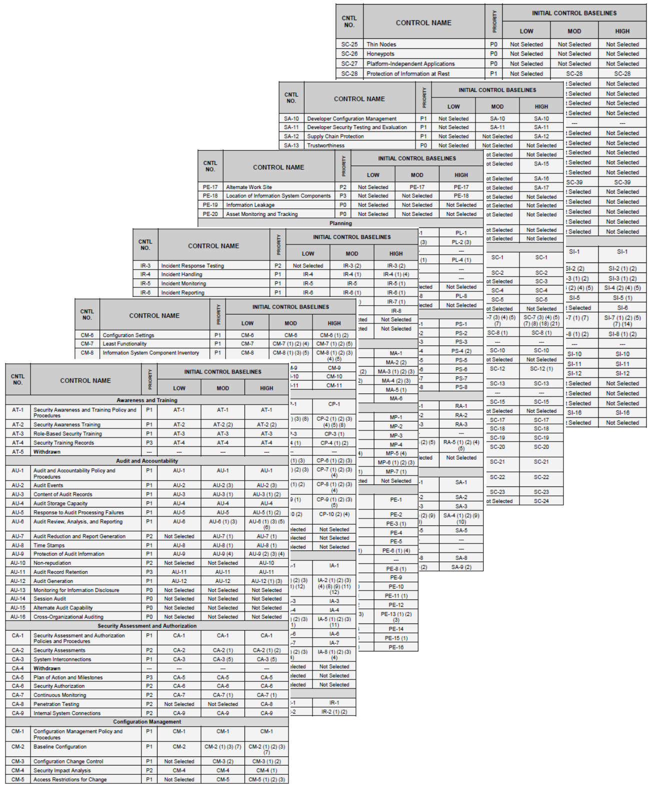
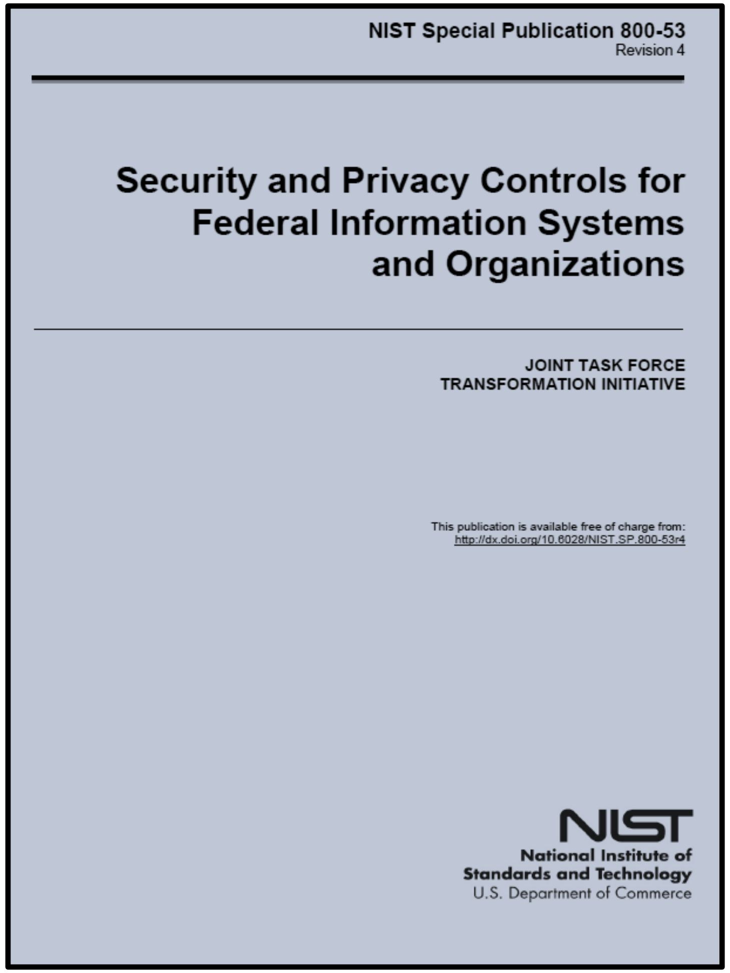


TABLE D-2: SECURITY CONTROL BASELINES[92]

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
	Access Control				
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5
AC-6	Least Privilege	P1	Not Selected	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)
AC-7	Unsuccessful Logon Attempts	P2	AC-7	AC-7	AC-7
AC-8	System Use Notification	P1	AC-8	AC-8	AC-8
AC-9	Previous Logon (Access) Notification	P0	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	P3	Not Selected	Not Selected	AC-10
AC-11	Session Lock	P3	Not Selected	AC-11 (1)	AC-11 (1)
AC-12	Session Termination	P2	Not Selected	AC-12	AC-12
AC-13	**Withdrawn**	---	---	---	---
AC-14	Permitted Actions without Identification or Authentication	P3	AC-14	AC-14	AC-14
AC-15	**Withdrawn**	---	---	---	---
AC-16	Security Attributes	P0	Not Selected	Not Selected	Not Selected
AC-17	Remote Access	P1	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)
AC-18	Wireless Access	P1	AC-18	AC-18 (1)	AC-18 (1) (4) (5)
AC-19	Access Control for Mobile Devices	P1	AC-19	AC-19 (5)	AC-19 (5)
AC-20	Use of External Information Systems	P1	AC-20	AC-20 (1) (2)	AC-20 (1) (2)
AC-21	Information Sharing	P2	Not Selected	AC-21	AC-21
AC-22	Publicly Accessible Content	P3	AC-22	AC-22	AC-22
AC-23	Data Mining Protection	P0	Not Selected	Not Selected	Not Selected
AC-24	Access Control Decisions	P0	Not Selected	Not Selected	Not Selected
AC-25	Reference Monitor	P0	Not Selected	Not Selected	Not Selected



AC-1



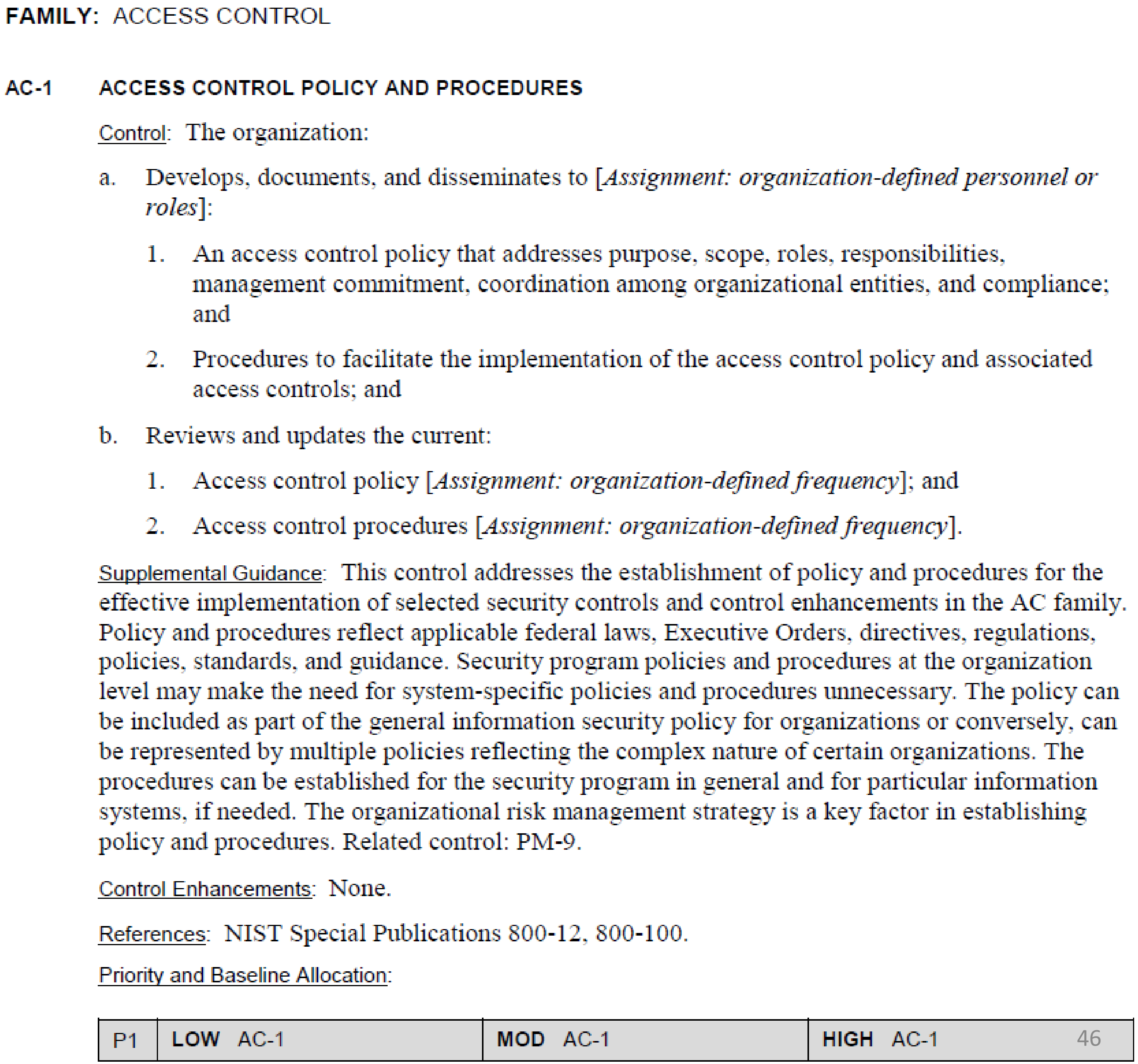
NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-53r4

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce



FAMILY: ACCESS CONTROL

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

   1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the access control policy and associated access controls; and

b. Reviews and updates the current:

   1. Access control policy [*Assignment: organization-defined frequency*]; and

   2. Access control procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

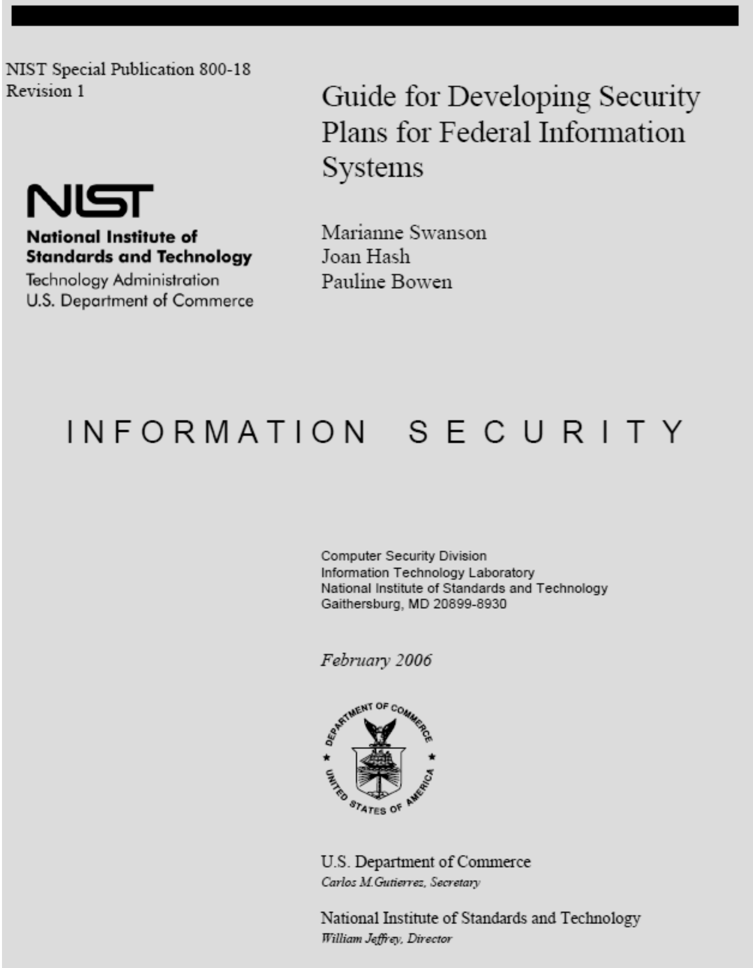
Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	**LOW** AC-1	**MOD** AC-1	**HIGH** AC-1

What kind of control is Access Control?



NIST Special Publication 800-18
Revision 1

Guide for Developing Security Plans for Federal Information Systems

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Marianne Swanson
Joan Hash
Pauline Bowen

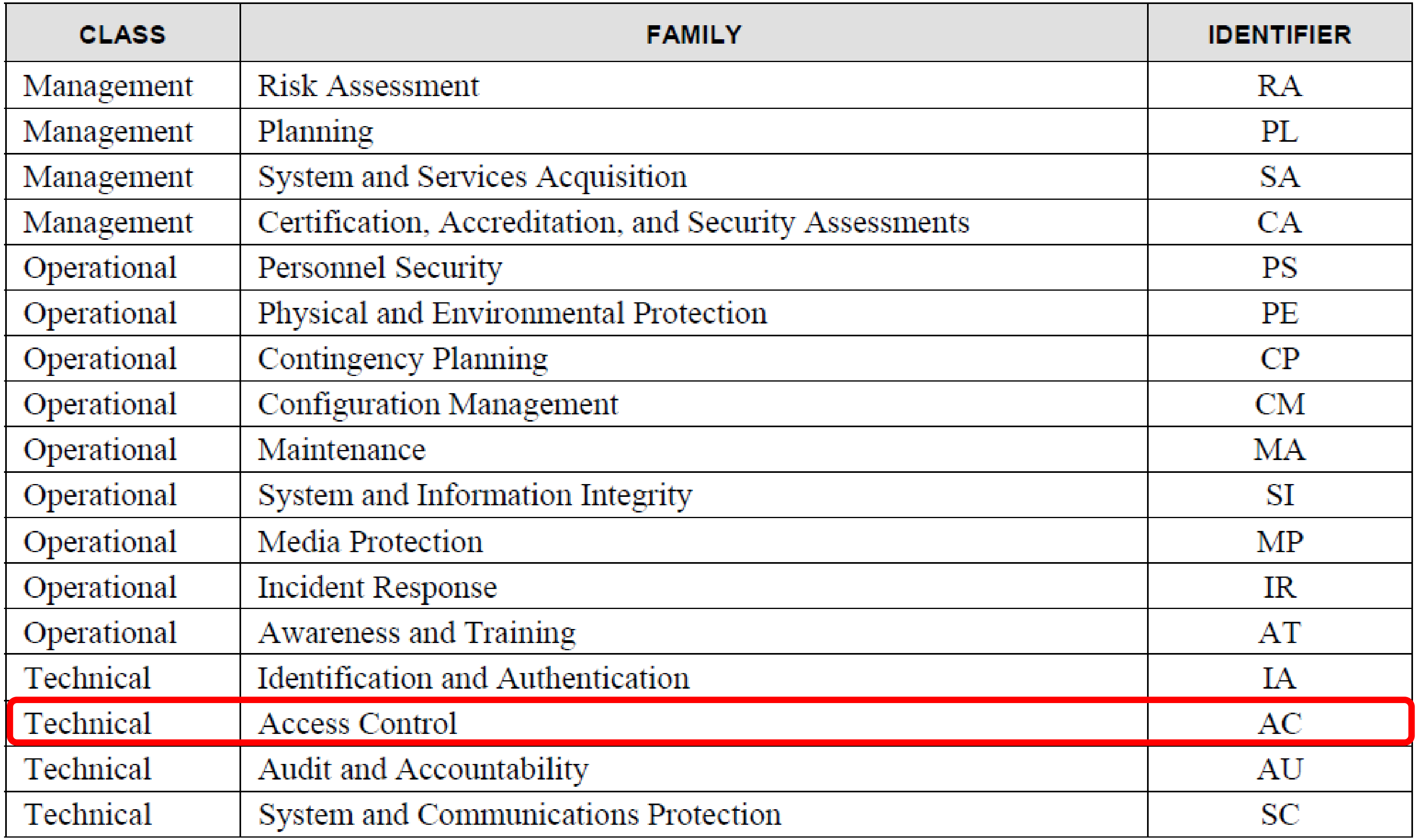
INFORMATION SECURITY

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

February 2006

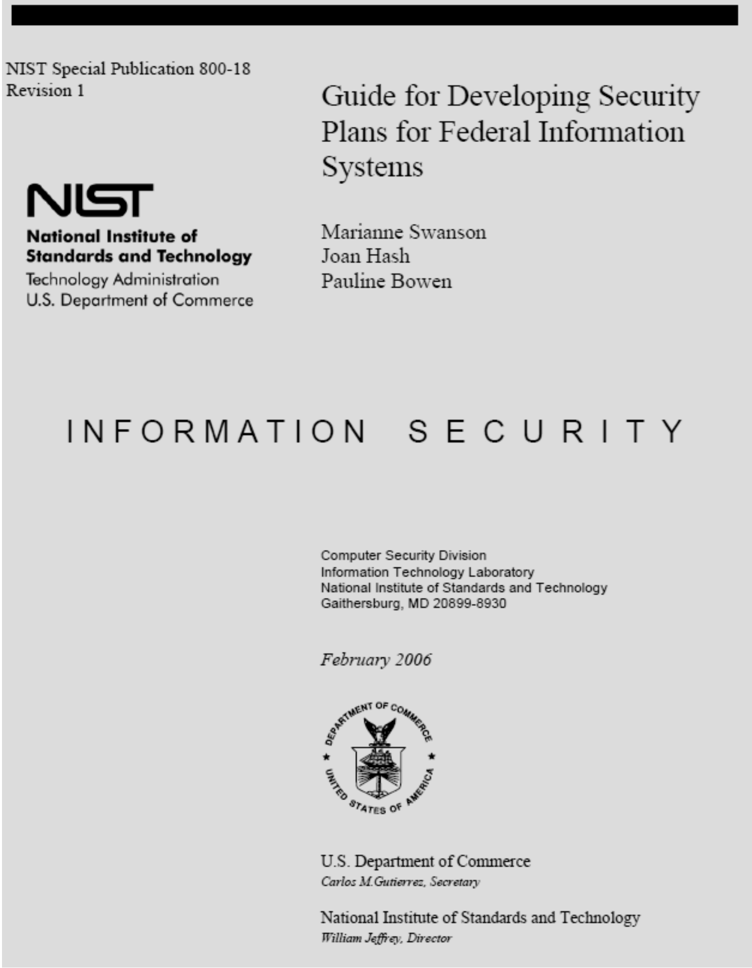
U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology
William Jeffrey, Director



CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and Security Assessments	CA
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency Planning	CP
Operational	Configuration Management	CM
Operational	Maintenance	MA
Operational	System and Information Integrity	SI
Operational	Media Protection	MP
Operational	Incident Response	IR
Operational	Awareness and Training	AT
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

Table 2: Security Control Class, Family, and Identifier



NIST Special Publication 800-18
Revision 1

Guide for Developing Security Plans for Federal Information Systems

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Marianne Swanson
Joan Hash
Pauline Bowen

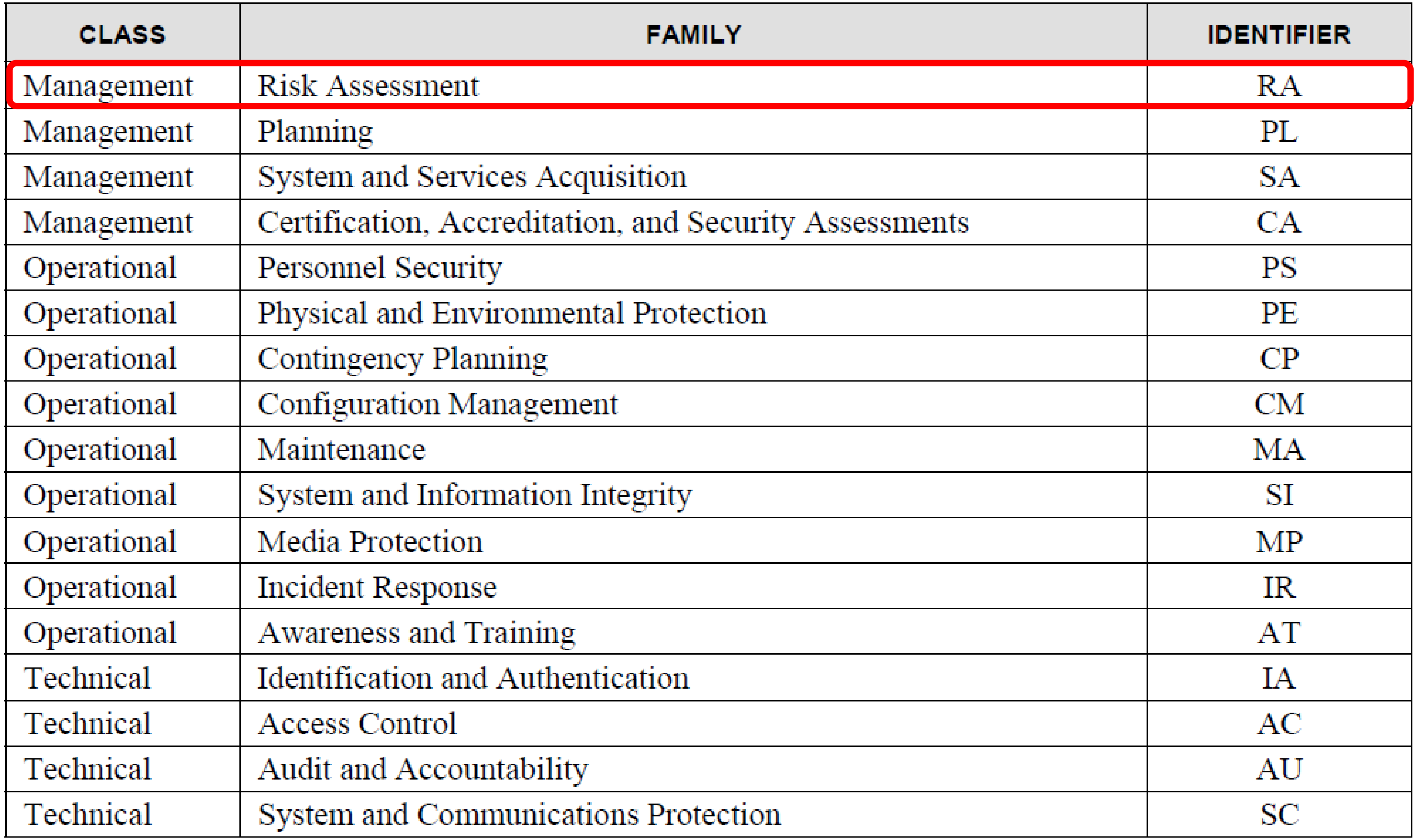
INFORMATION SECURITY

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

February 2006

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

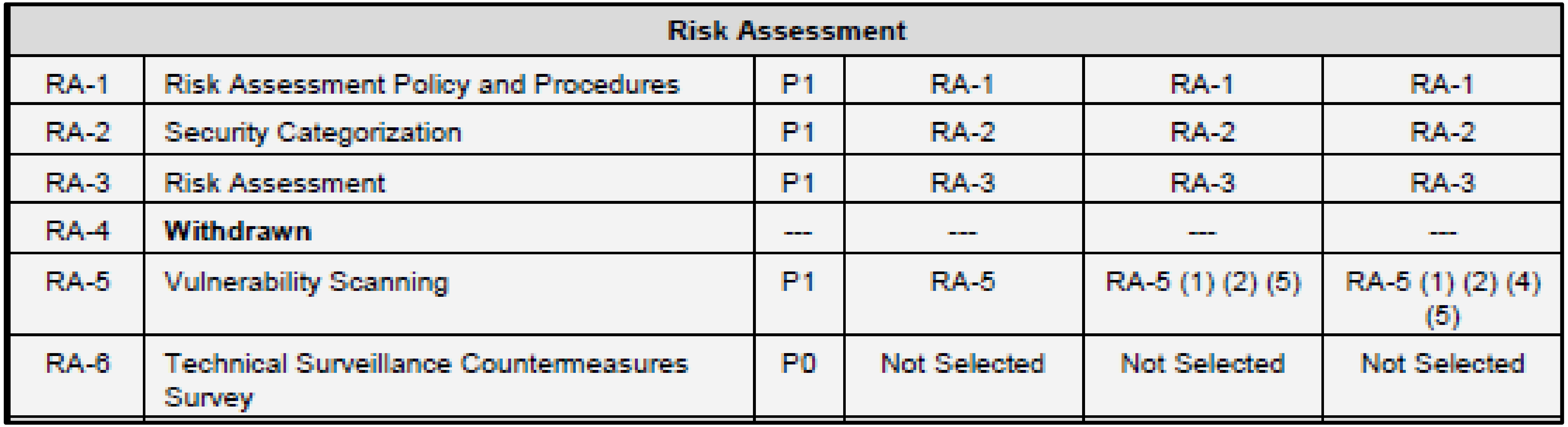
National Institute of Standards and Technology
William Jeffrey, Director



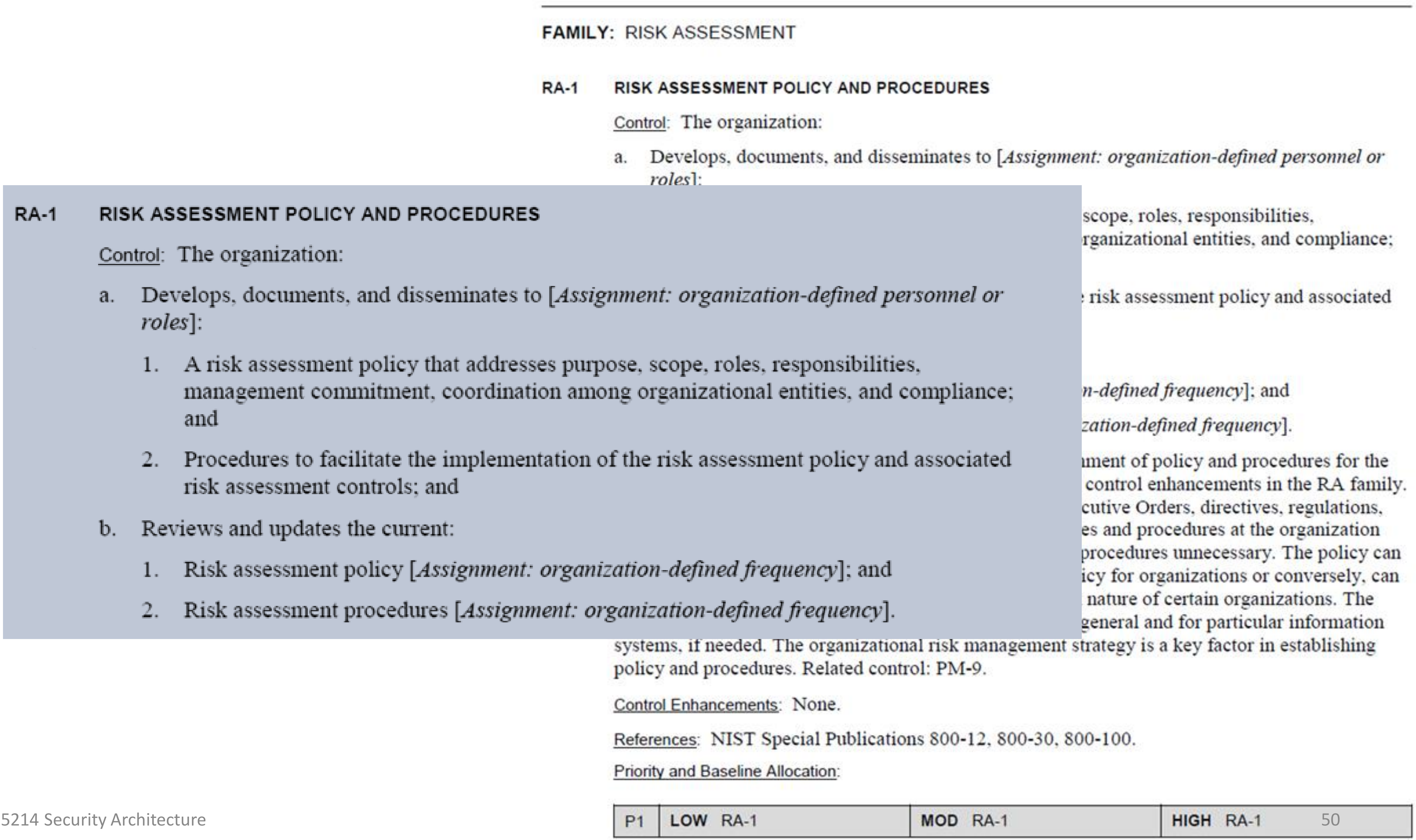
CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and Security Assessments	CA
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency Planning	CP
Operational	Configuration Management	CM
Operational	Maintenance	MA
Operational	System and Information Integrity	SI
Operational	Media Protection	MP
Operational	Incident Response	IR
Operational	Awareness and Training	AT
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

Table 2: Security Control Class, Family, and Identifier

Risk Assessment (RA) Controls



Risk Assessment					
RA-1	Risk Assessment Policy and Procedures	P1	RA-1	RA-1	RA-1
RA-2	Security Categorization	P1	RA-2	RA-2	RA-2
RA-3	Risk Assessment	P1	RA-3	RA-3	RA-3
RA-4	**Withdrawn**	---	---	---	---
RA-5	Vulnerability Scanning	P1	RA-5	RA-5 (1) (2) (5)	RA-5 (1) (2) (4) (5)
RA-6	Technical Surveillance Countermeasures Survey	P0	Not Selected	Not Selected	Not Selected



FAMILY: RISK ASSESSMENT

RA-1 RISK ASSESSMENT POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and

b. Reviews and updates the current:

1. Risk assessment policy [*Assignment: organization-defined frequency*]; and
2. Risk assessment procedures [*Assignment: organization-defined frequency*].

RA-1 RISK ASSESSMENT POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

scope, roles, responsibilities,
rganizational entities, and compliance;

risk assessment policy and associated

n-defined frequency]; and

zation-defined frequency].

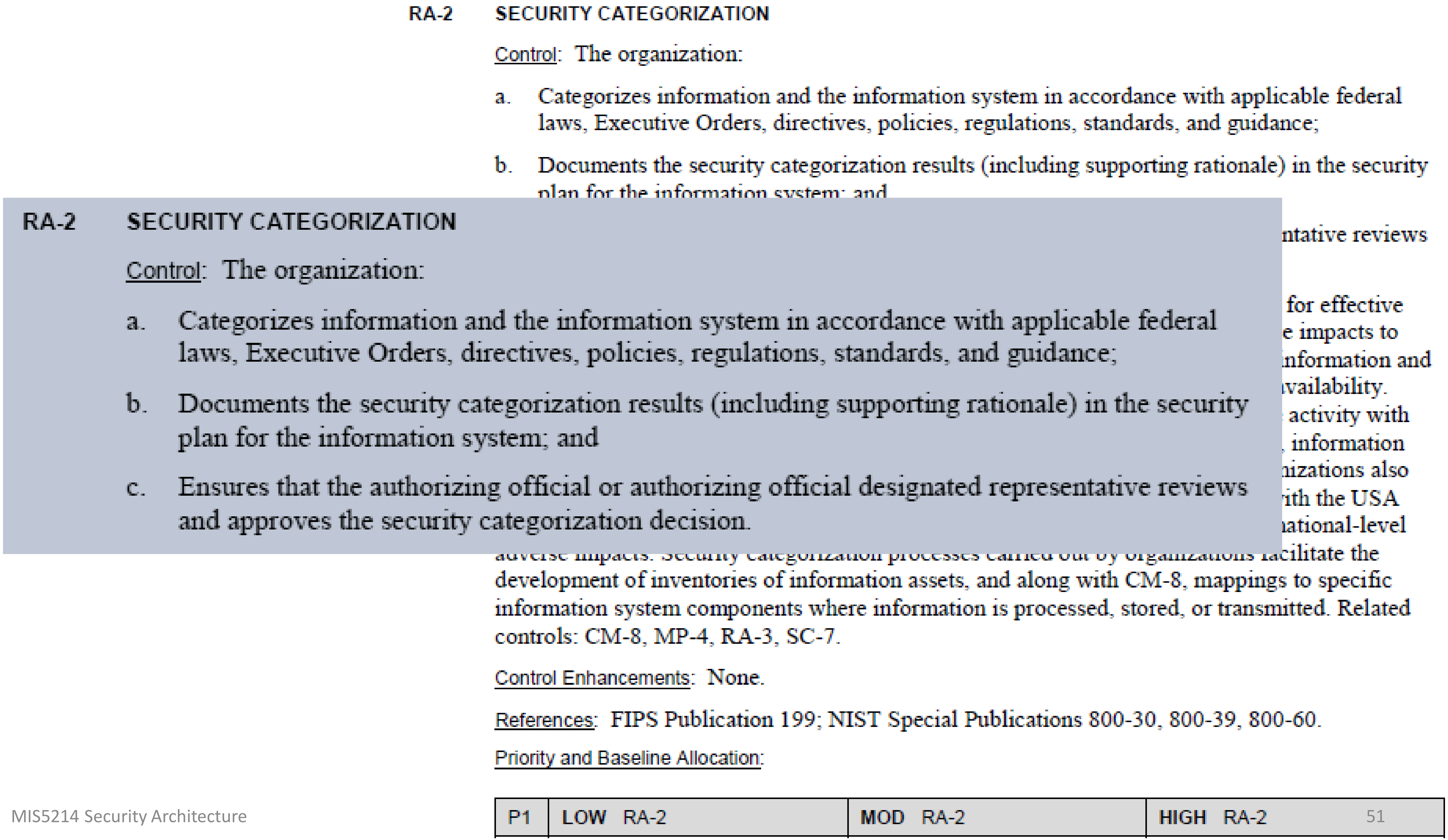
ment of policy and procedures for the
control enhancements in the RA family.
cutive Orders, directives, regulations,
es and procedures at the organization
procedures unnecessary. The policy can
icy for organizations or conversely, can
nature of certain organizations. The
general and for particular information
systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-30, 800-100.

Priority and Baseline Allocation:

P1	**LOW** RA-1	**MOD** RA-1	**HIGH** RA-1



RA-2 SECURITY CATEGORIZATION

Control: The organization:

a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and

c. Ensures that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

RA-2 SECURITY CATEGORIZATION

Control: The organization:

a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and

ntative reviews

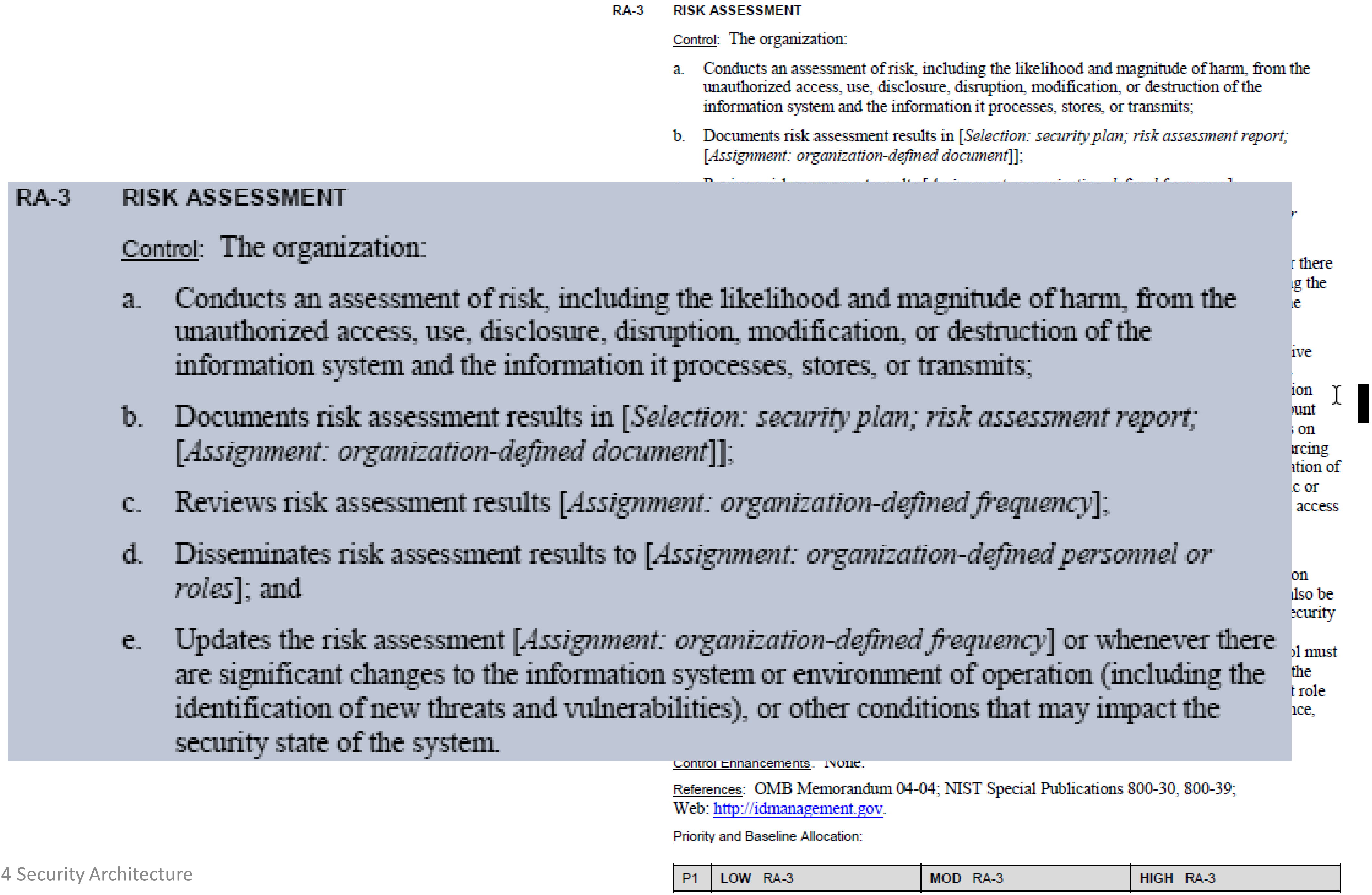
for effective
e impacts to
information and
vailability.
activity with
, information
nizations also
ith the USA
national-level
adverse impacts. Security categorization processes carried out by organizations facilitate the development of inventories of information assets, and along with CM-8, mappings to specific information system components where information is processed, stored, or transmitted. Related controls: CM-8, MP-4, RA-3, SC-7.

Control Enhancements: None.

References: FIPS Publication 199; NIST Special Publications 800-30, 800-39, 800-60.

Priority and Baseline Allocation:

P1	LOW RA-2	MOD RA-2	HIGH RA-2



RA-3 RISK ASSESSMENT

Control: The organization:

a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;

b. Documents risk assessment results in [*Selection: security plan; risk assessment report;* [*Assignment: organization-defined document*]];

c. Reviews risk assessment results [*Assignment: organization-defined frequency*];

d. Disseminates risk assessment results to [*Assignment: organization-defined personnel or roles*]; and

e. Updates the risk assessment [*Assignment: organization-defined frequency*] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

RA-3 RISK ASSESSMENT

Control: The organization:

a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;

b. Documents risk assessment results in [*Selection: security plan; risk assessment report;* [*Assignment: organization-defined document*]];

r there
g the
e

ive

ion
unt
on
rcing
ation of
c or
access

on
also be
ecurity

ol must
the
t role
nce,

Control Enhancements: None.

References: OMB Memorandum 04-04; NIST Special Publications 800-30, 800-39; Web: http://idmanagement.gov.

Priority and Baseline Allocation:

P1	LOW RA-3	MOD RA-3	HIGH RA-3

Exercise

1. Using your favorite search engine…
   - Find an organization’s IT risk assessment policy and procedures
     - *Assess how well the policy meets requirements of RA-1*
     - *Assess how well the procedures meet RA2 and RA3*

2. Return to class discussion
3. Present your findings

Agenda

- ✓NIST Risk Management Framework and FIPS 199
- ✓Use of NIST SP 800-60 Volume 1 and Volume 2
- ✓*Exercise – Determine and finalize impact levels*
- ✓*Exercise – Determine Information and Information System Types and provisional security categorization*
- ✓Security Control Baselines – review
  - ✓FIPS 200 and NIST 800-53 Security Control Baselines
  - ✓Security Control Families
- ✓Risk Assessment Controls
- ✓Team Exercise *Find and assess risk assessment policy*

Unit #3

MIS5214

Planning and Policy