Managing Enterprise Cybersecurity MIS 4596

Class 3

Agenda

- National Institute of Standards and Technology (NIST)
  - Cybersecurity Framework
  - Risk Management Framework
- Applying the NIST Risk Management Framework
- Milestone 1 Assignment
- Prepare for next time to take 100 Digits of Pi Quiz

Federal Information Security Management Act (FISMA) of 2002
Federal Information Security Modernization Act (FISMA) of 2014

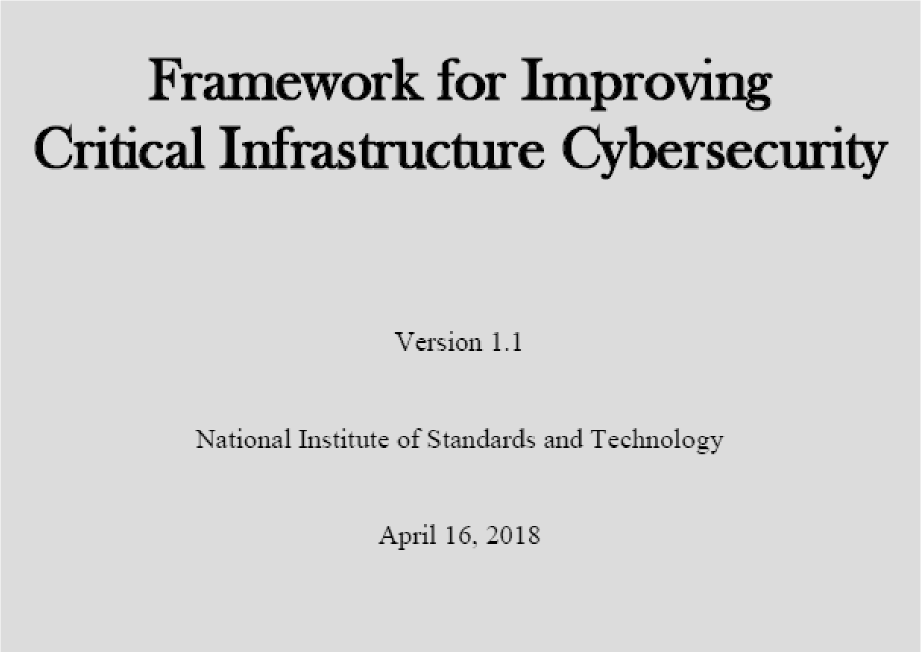
Recognizes importance of information security to the economy and national security

- Requires each government organization to provide information security for information and information systems supporting their operations and assets
    - *Including those provided or managed by another agency, contractors, or other sources*
- Made NIST responsible for developing standards, guidelines, and associated methods and techniques for providing adequate information security for all agency operations and assets (excluding national security systems)

https://www.dhs.gov/fisma

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

NIST's "Cybersecurity Framework"

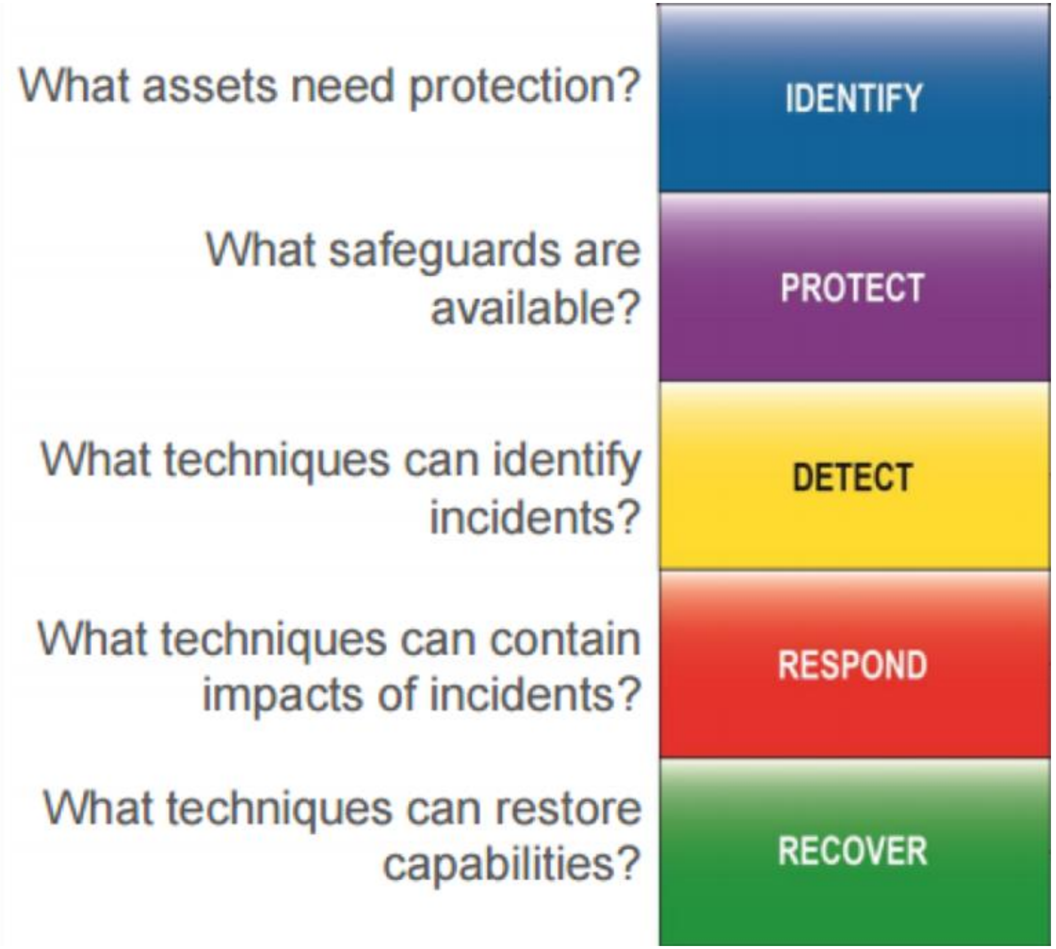


Framework for Improving Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018



What assets need protection? — IDENTIFY

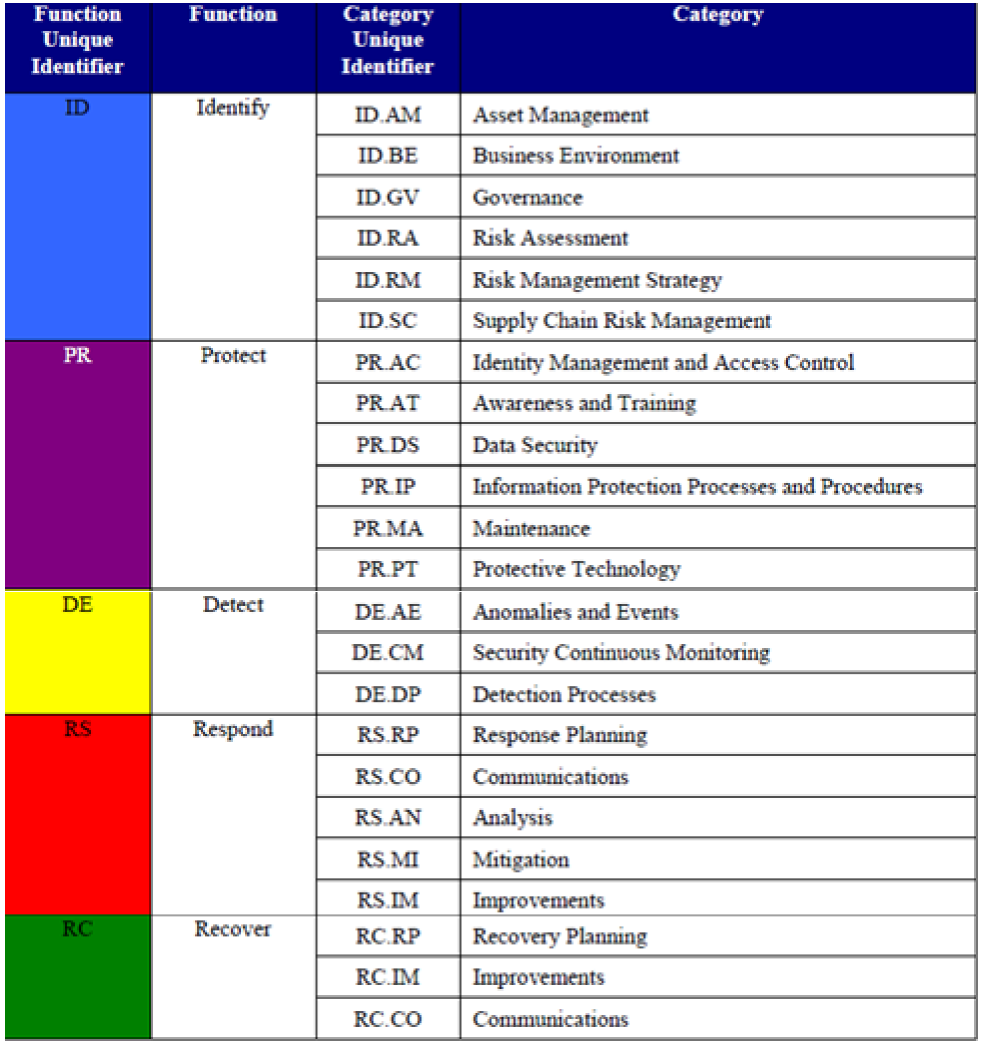
What safeguards are available? — PROTECT

What techniques can identify incidents? — DETECT

What techniques can contain impacts of incidents? — RESPOND

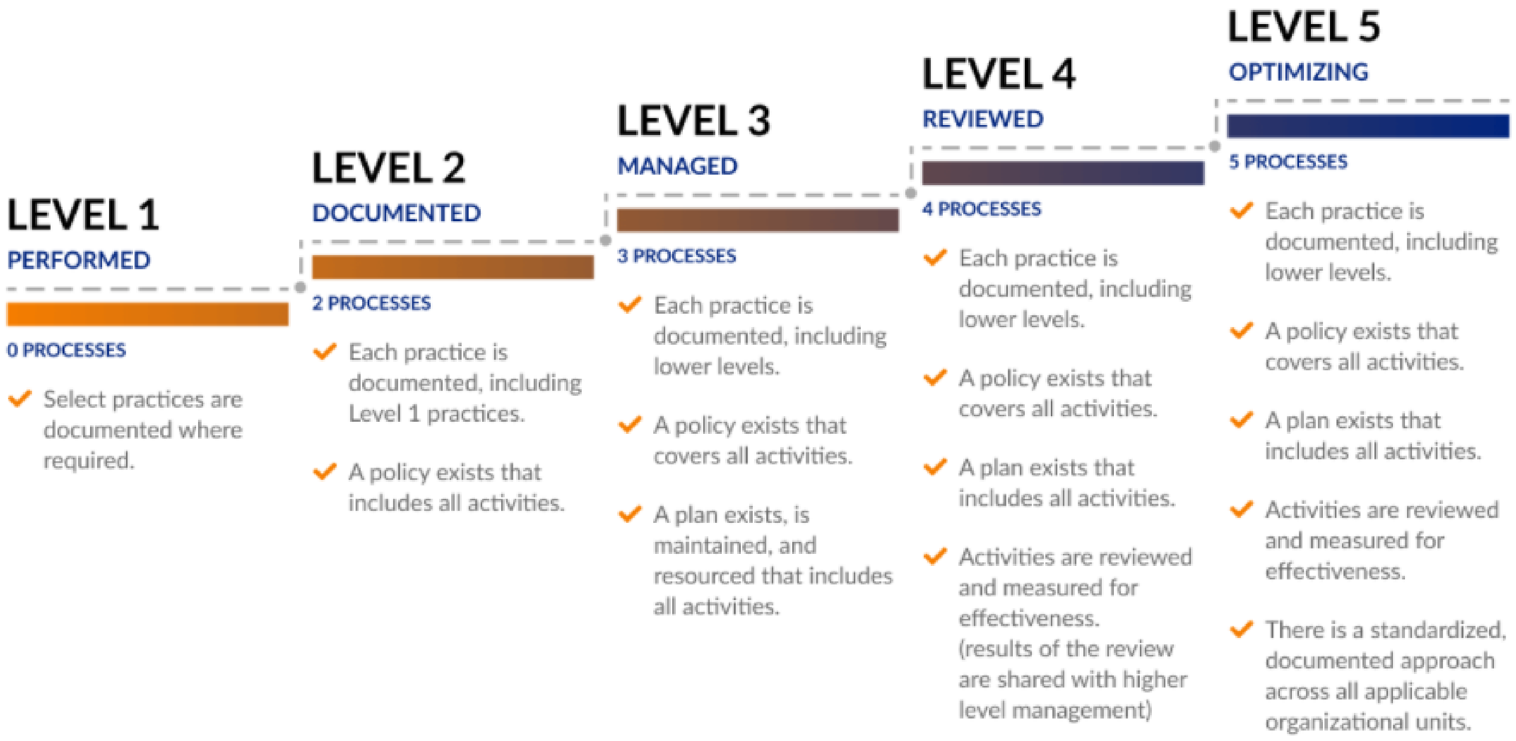
What techniques can restore capabilities? — RECOVER

NIST Cybersecurity Framework



Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Cybersecurity Maturity Model Certification (CMMC) levels



LEVEL 1
PERFORMED
0 PROCESSES
✓ Select practices are documented where required.

LEVEL 2
DOCUMENTED
2 PROCESSES
✓ Each practice is documented, including Level 1 practices.
✓ A policy exists that includes all activities.

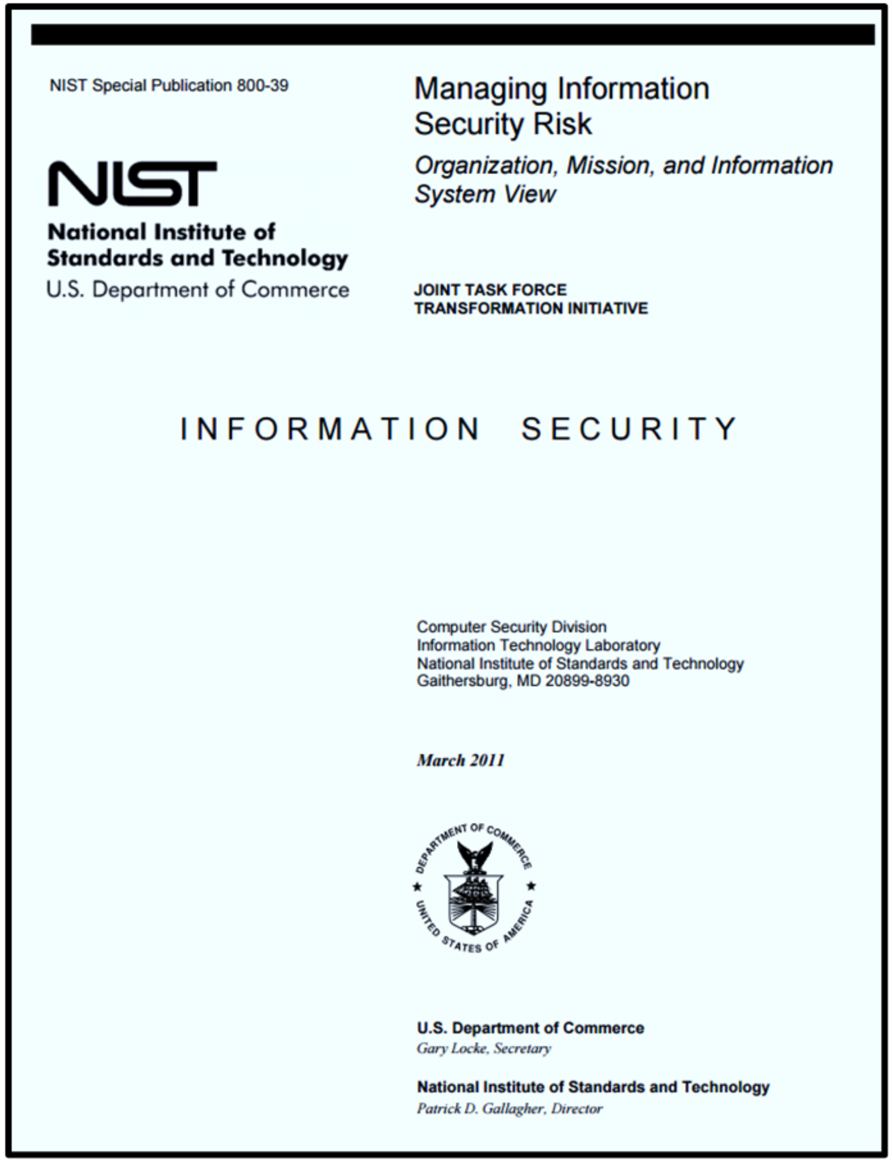
LEVEL 3
MANAGED
3 PROCESSES
✓ Each practice is documented, including lower levels.
✓ A policy exists that covers all activities.
✓ A plan exists, is maintained, and resourced that includes all activities.

LEVEL 4
REVIEWED
4 PROCESSES
✓ Each practice is documented, including lower levels.
✓ A policy exists that covers all activities.
✓ A plan exists that includes all activities.
✓ Activities are reviewed and measured for effectiveness. (results of the review are shared with higher level management)

LEVEL 5
OPTIMIZING
5 PROCESSES
✓ Each practice is documented, including lower levels.
✓ A policy exists that covers all activities.
✓ A plan exists that includes all activities.
✓ Activities are reviewed and measured for effectiveness.
✓ There is a standardized, documented approach across all applicable organizational units.

Is used to assess an organization's cybersecurity capability maturity level, and recommend steps for improvement

NIST's Risk Management Framework



NIST Special Publication 800-39

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

Managing Information Security Risk

Organization, Mission, and Information System View

JOINT TASK FORCE TRANSFORMATION INITIATIVE

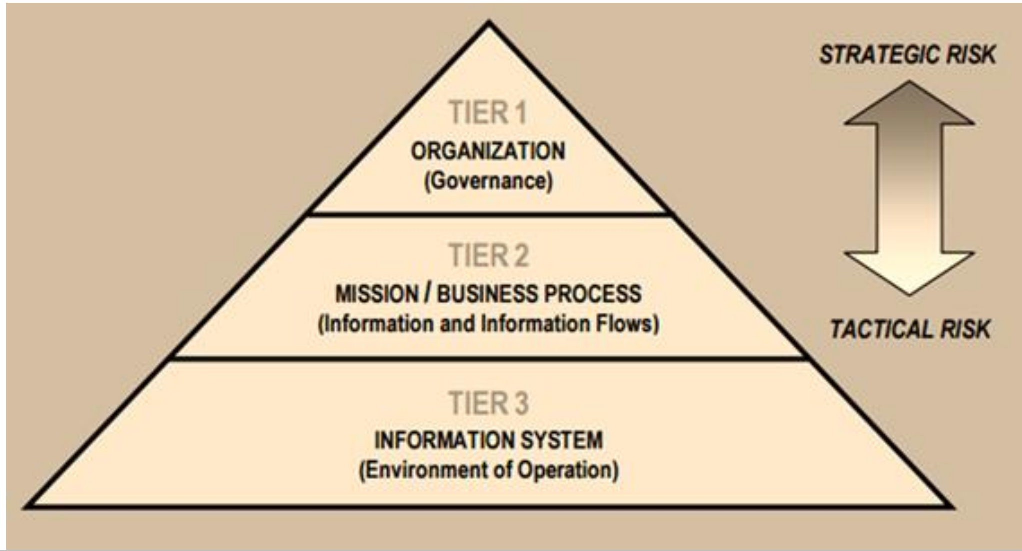
INFORMATION SECURITY

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

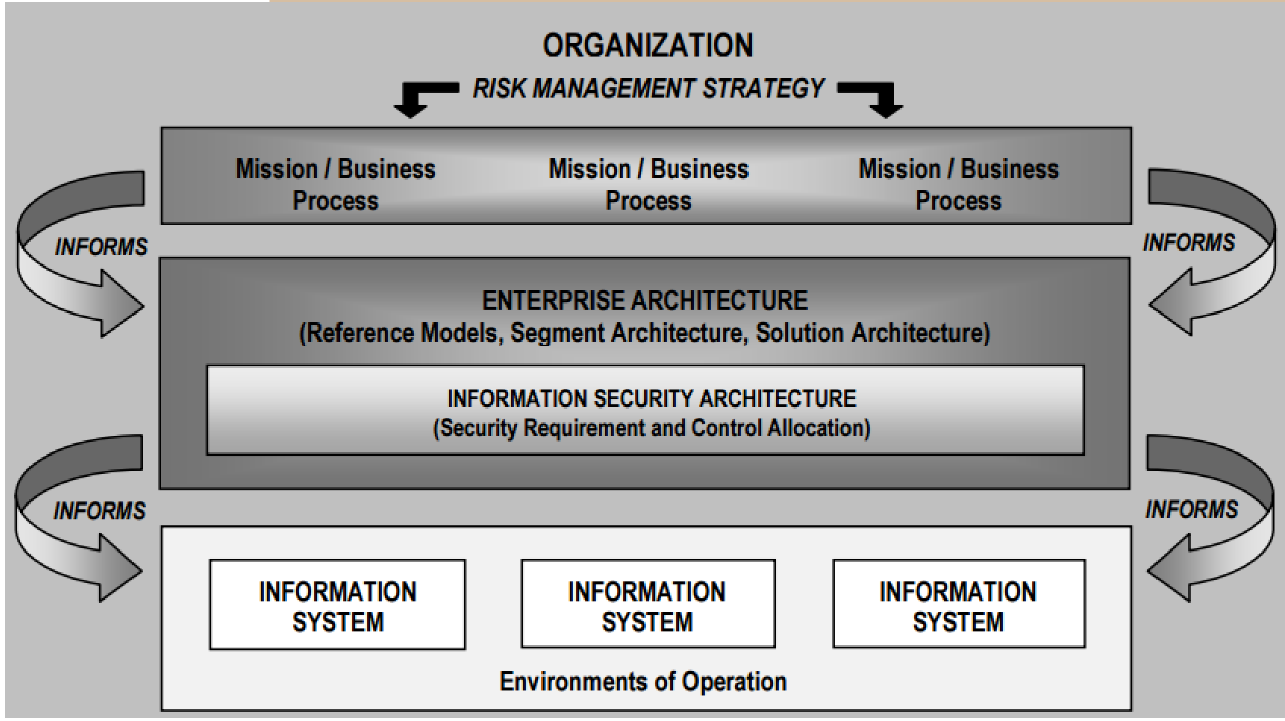
March 2011

U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Director



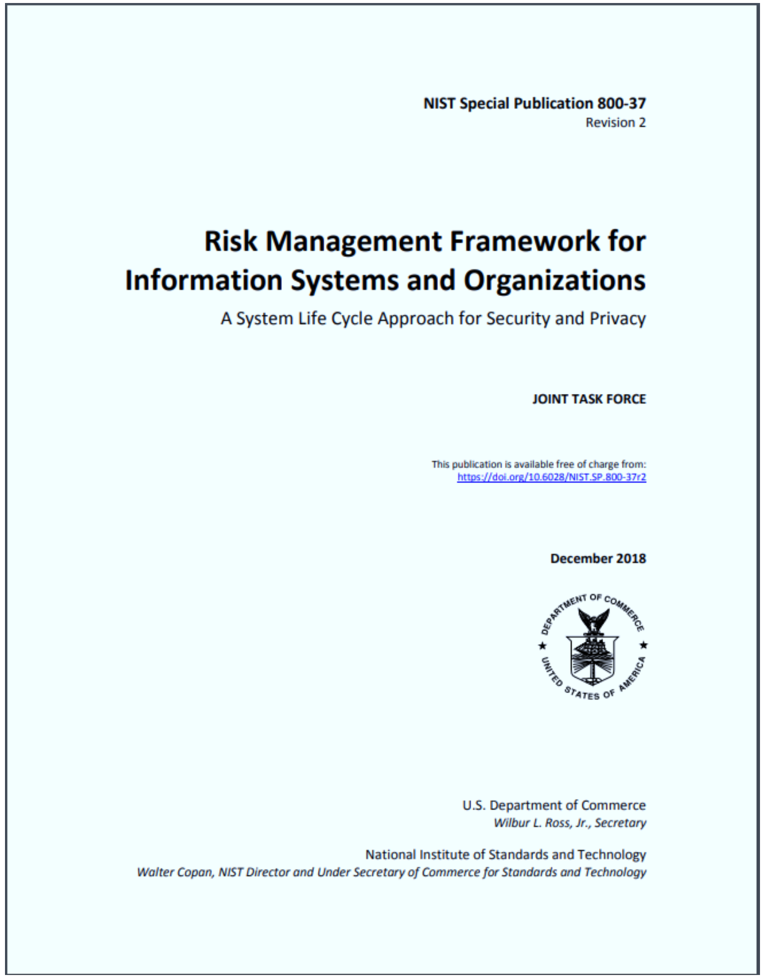
STRATEGIC RISK
TIER 1
ORGANIZATION
(Governance)
TIER 2
MISSION / BUSINESS PROCESS
(Information and Information Flows)
TIER 3
INFORMATION SYSTEM
(Environment of Operation)
TACTICAL RISK



ORGANIZATION
RISK MANAGEMENT STRATEGY
Mission / Business Process
Mission / Business Process
Mission / Business Process
INFORMS
INFORMS
ENTERPRISE ARCHITECTURE
(Reference Models, Segment Architecture, Solution Architecture)
INFORMATION SECURITY ARCHITECTURE
(Security Requirement and Control Allocation)
INFORMS
INFORMS
INFORMATION SYSTEM
INFORMATION SYSTEM
INFORMATION SYSTEM
Environments of Operation

Security Categorization & Selecting a Baseline of Cybersecurity Risk Controls

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



NIST Special Publication 800-37
Revision 2

Risk Management Framework for Information Systems and Organizations

A System Life Cycle Approach for Security and Privacy

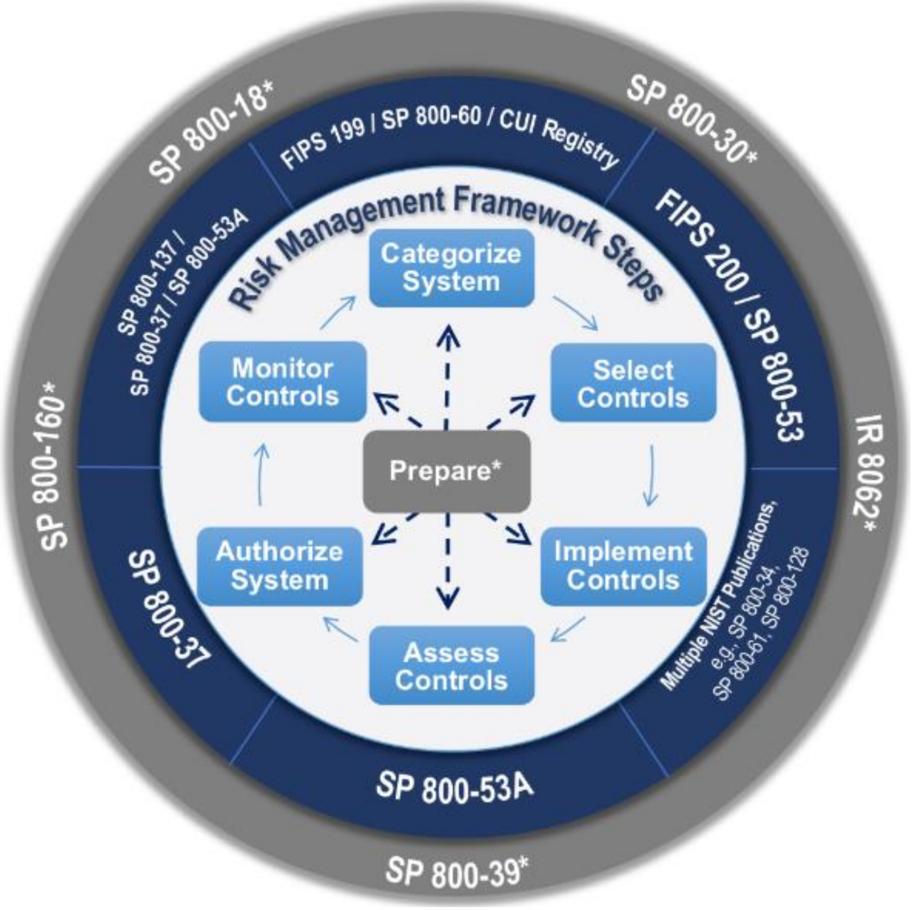
JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-37r2

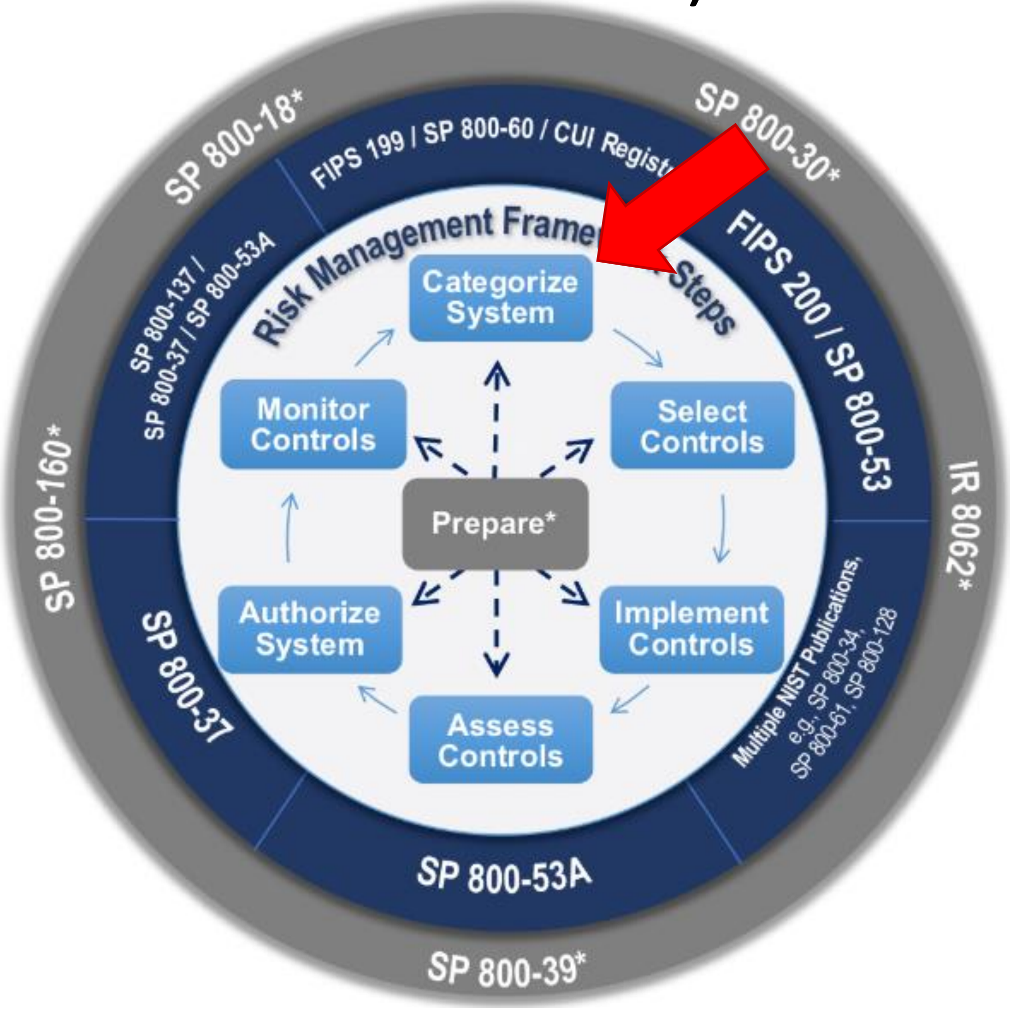
December 2018

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology



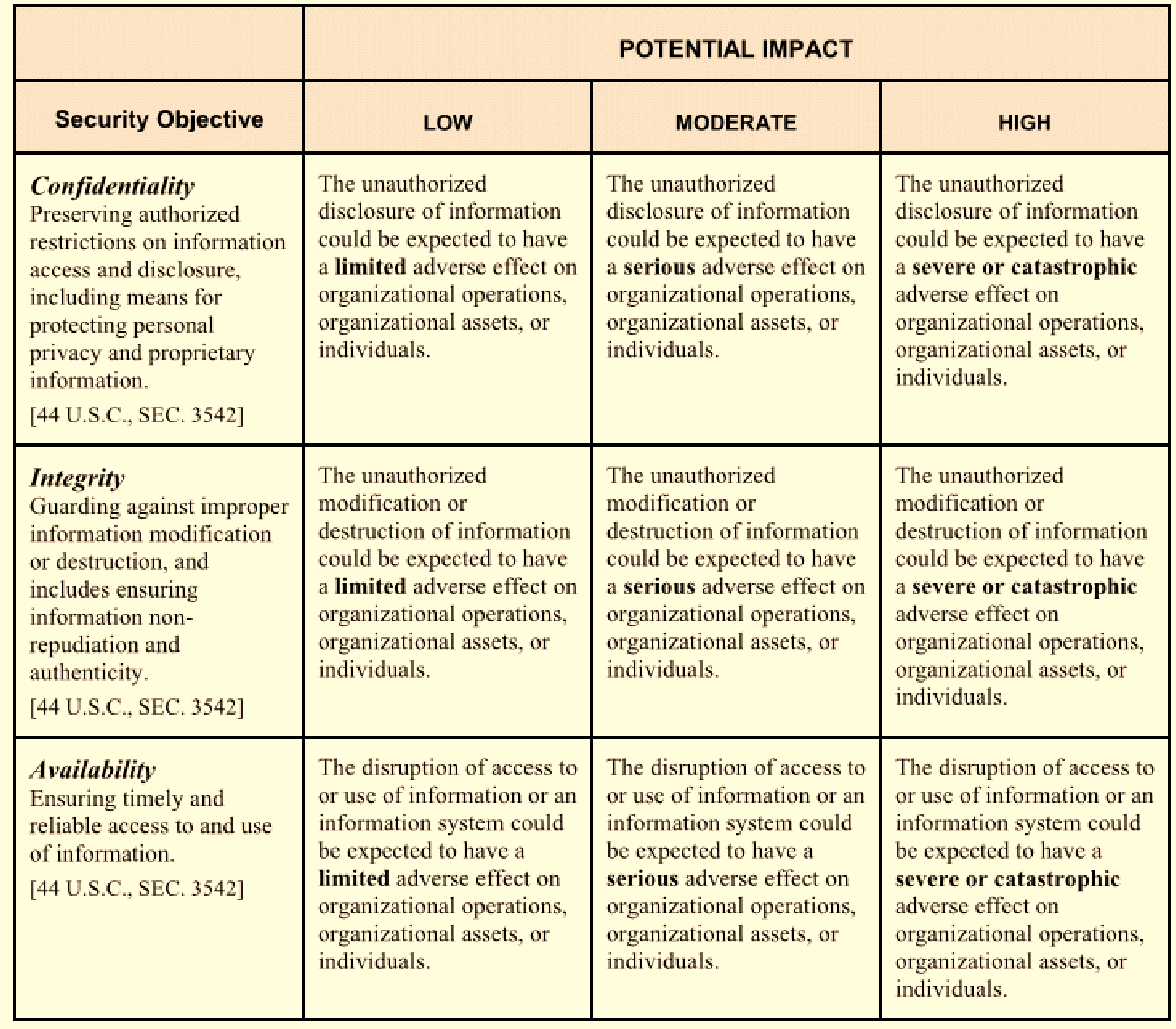
1st Step in cybersecurity is security categorization (i.e. risk assessment)



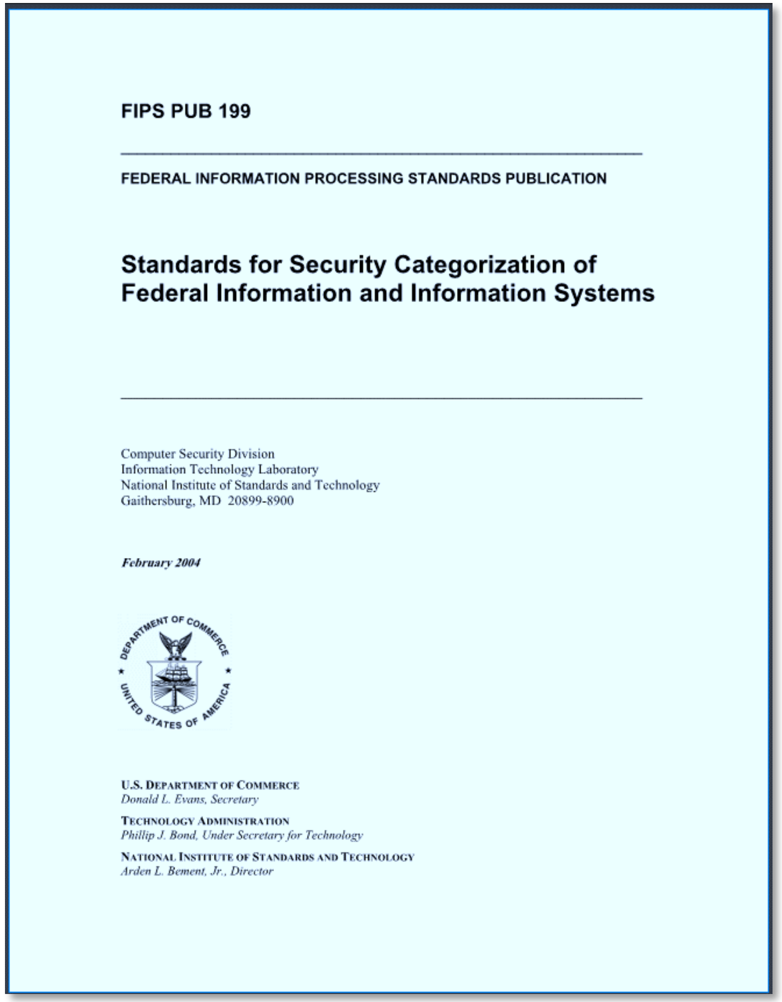
i. Inventory the data content of the information system

ii. Determine the security categorization of the information based on potential impacts a breach of confidentiality, integrity and availability will have on organizational operations, assets, or individuals based FIPS 199 standard

Risk is based on impact of a security breach



	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.



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

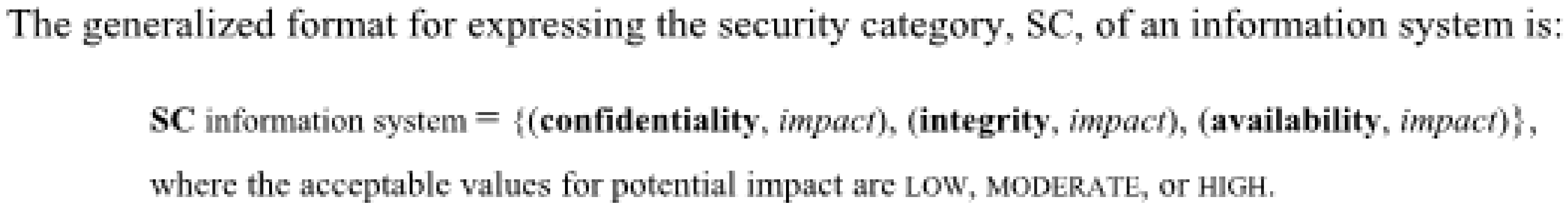
TECHNOLOGY ADMINISTRATION
Phillip J. Bond, Under Secretary for Technology

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

In the Risk Management Framework (RMF) likelihood of a breach is treated as 100%

FIPS Pub 199 Standards for Security Categorization

Low: Limited adverse effect
Medium: Serious adverse effect
High: Severe or catastrophic adverse effect

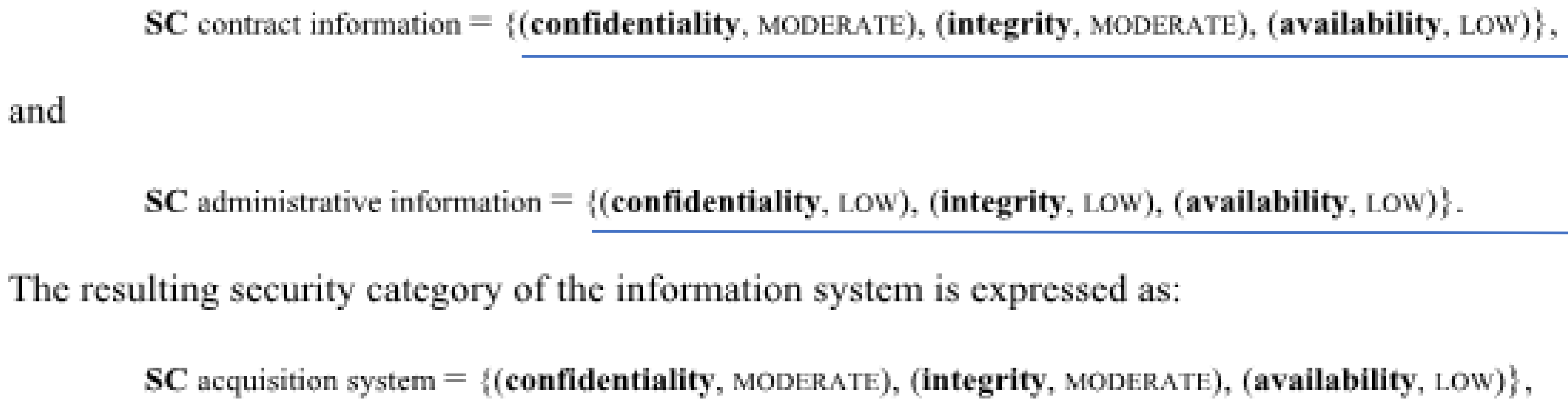


The generalized format for expressing the security category, SC, of an information system is:

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

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

Example with multiple information types:



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

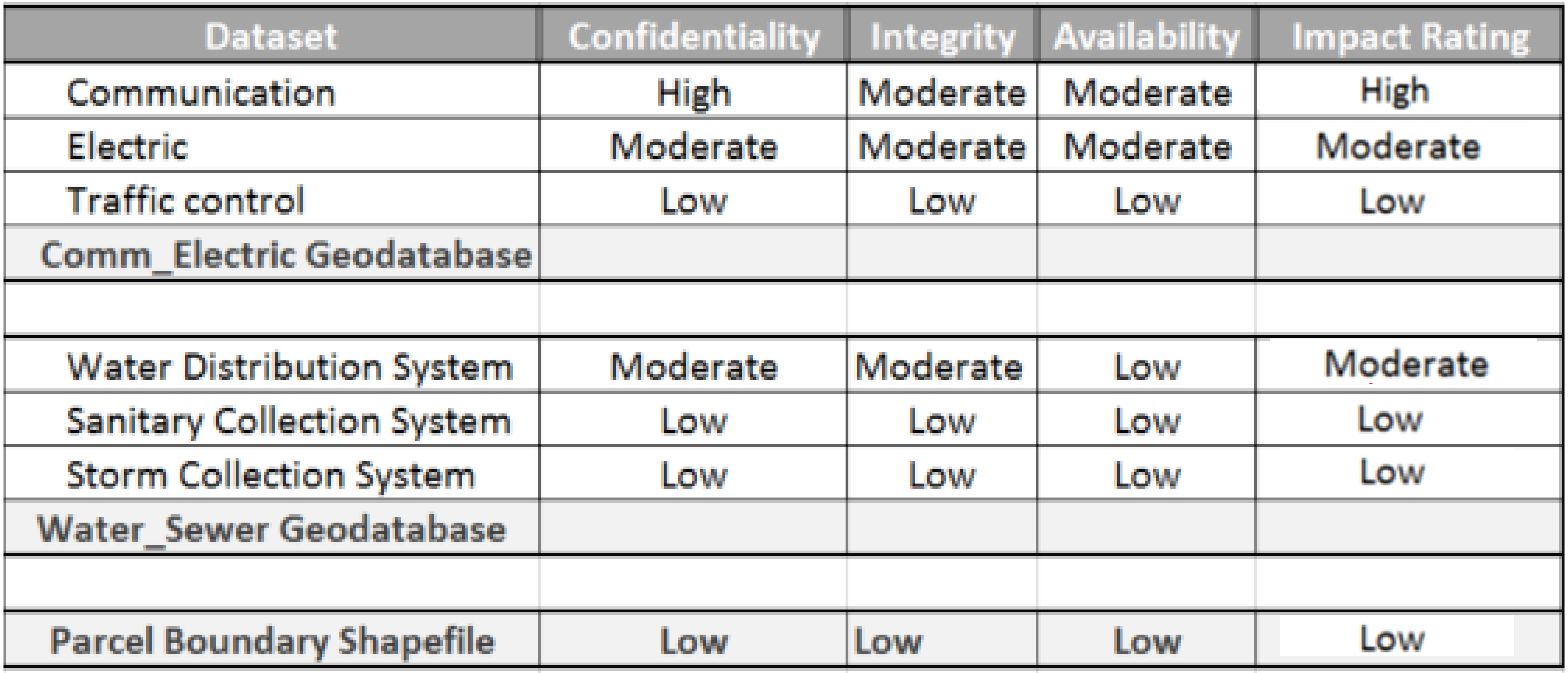
and

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

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

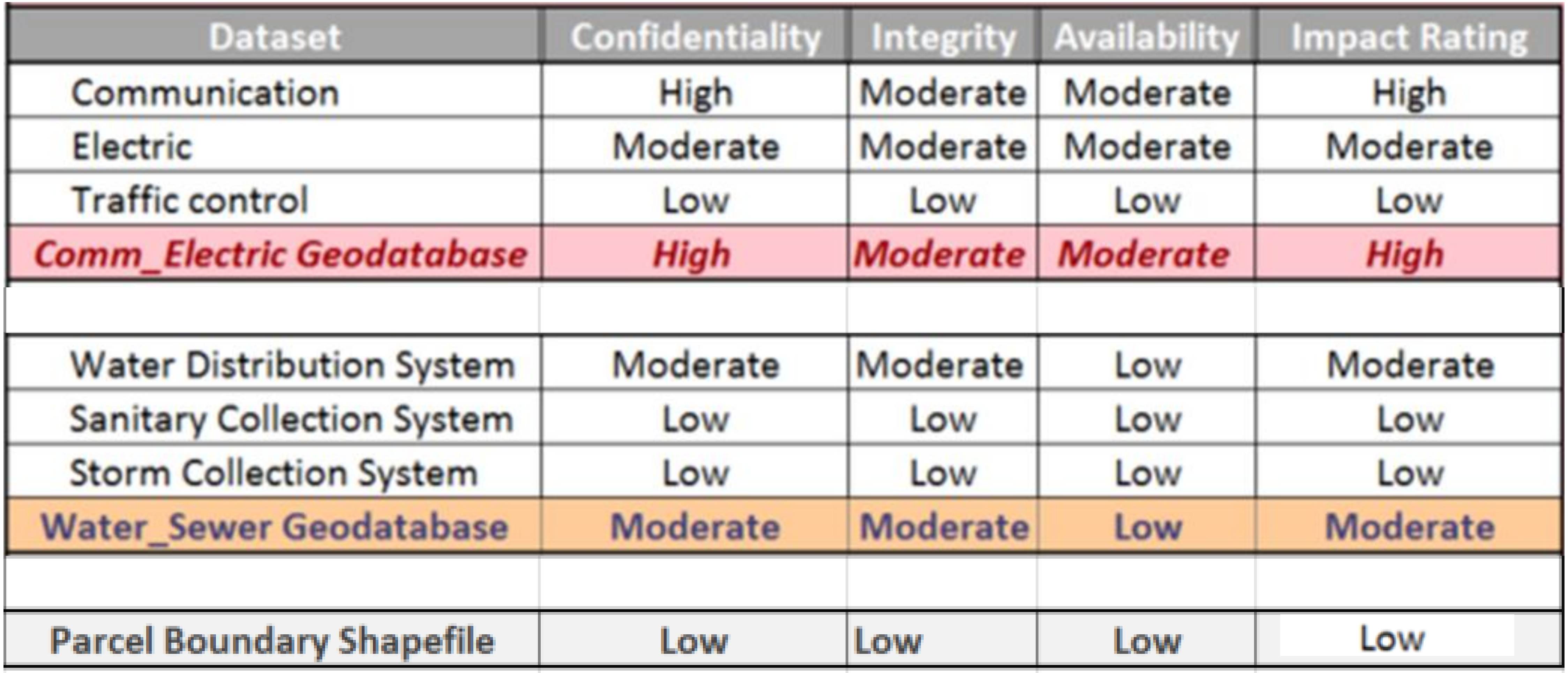
SC acquisition system = {(**confidentiality**, MODERATE), (**integrity**, MODERATE), (**availability**, LOW)}, = MODERATE rating

What are the security categorizations of these datasets?



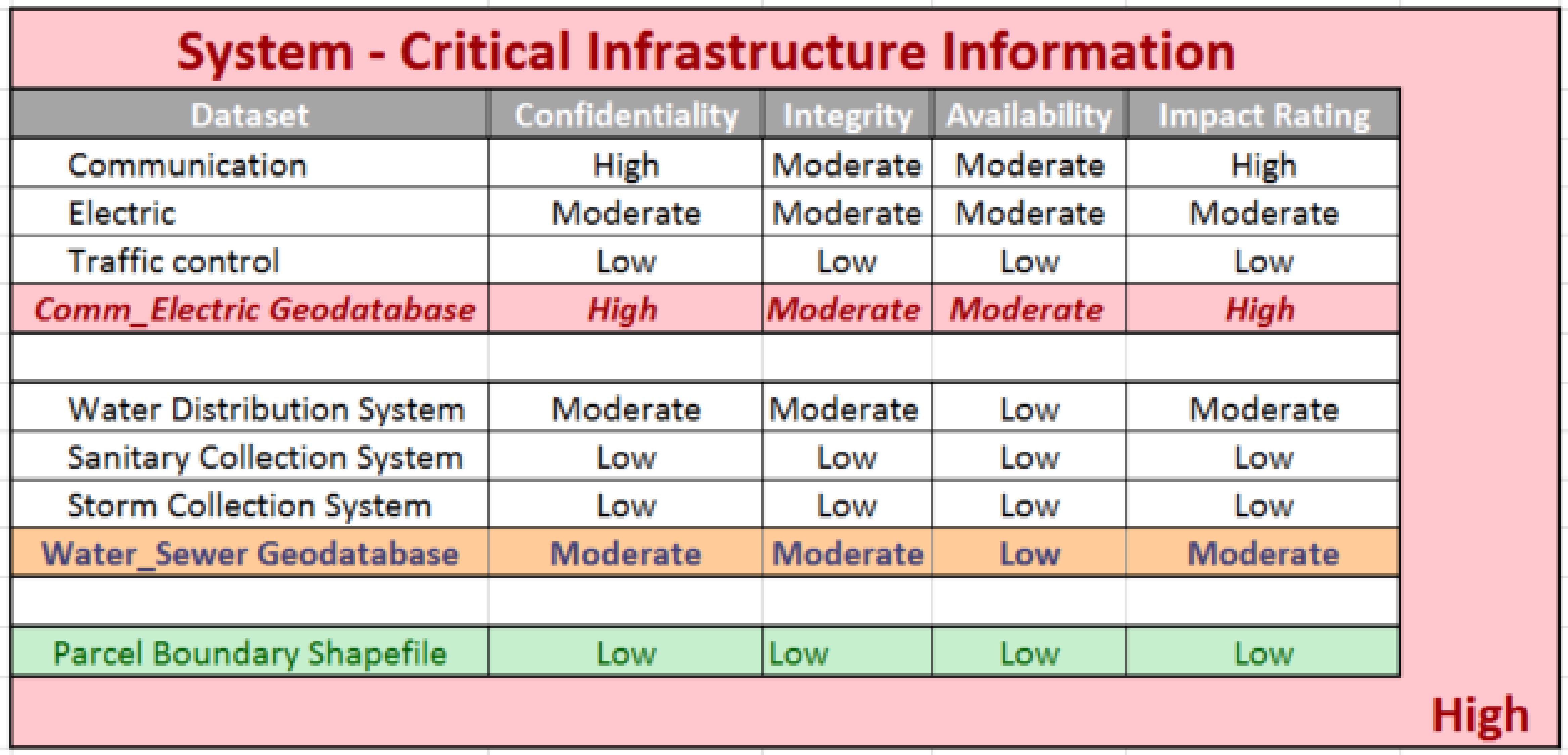
Dataset	Confidentiality	Integrity	Availability	Impact Rating
Communication	High	Moderate	Moderate	High
Electric	Moderate	Moderate	Moderate	Moderate
Traffic control	Low	Low	Low	Low
Comm_Electric Geodatabase				
Water Distribution System	Moderate	Moderate	Low	Moderate
Sanitary Collection System	Low	Low	Low	Low
Storm Collection System	Low	Low	Low	Low
Water_Sewer Geodatabase				
Parcel Boundary Shapefile	Low	Low	Low	Low

#*What are the security categorizations of the geodatabases?*



Dataset	Confidentiality	Integrity	Availability	Impact Rating
Communication	High	Moderate	Moderate	High
Electric	Moderate	Moderate	Moderate	Moderate
Traffic control	Low	Low	Low	Low
Comm_Electric Geodatabase	***High***	***Moderate***	***Moderate***	***High***
Water Distribution System	Moderate	Moderate	Low	Moderate
Sanitary Collection System	Low	Low	Low	Low
Storm Collection System	Low	Low	Low	Low
Water_Sewer Geodatabase	**Moderate**	**Moderate**	**Low**	**Moderate**
Parcel Boundary Shapefile	**Low**	**Low**	**Low**	**Low**

What is the overall security categorization of the information system containing these datasets?



System - Critical Infrastructure Information

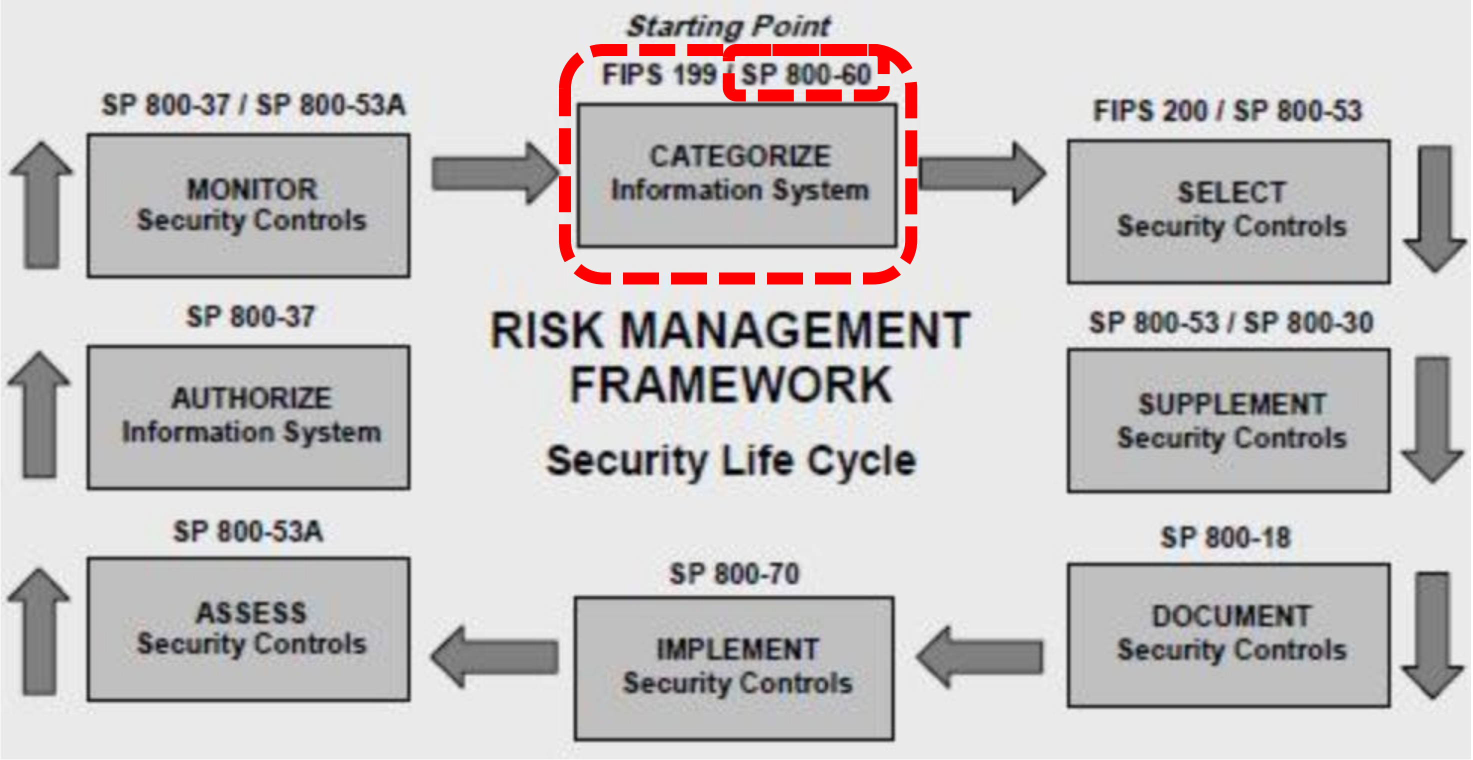
Dataset	Confidentiality	Integrity	Availability	Impact Rating
Communication	High	Moderate	Moderate	High
Electric	Moderate	Moderate	Moderate	Moderate
Traffic control	Low	Low	Low	Low
Comm_Electric Geodatabase	***High***	***Moderate***	***Moderate***	***High***
Water Distribution System	Moderate	Moderate	Low	Moderate
Sanitary Collection System	Low	Low	Low	Low
Storm Collection System	Low	Low	Low	Low
Water_Sewer Geodatabase	**Moderate**	**Moderate**	**Low**	**Moderate**
Parcel Boundary Shapefile	Low	Low	Low	Low

High

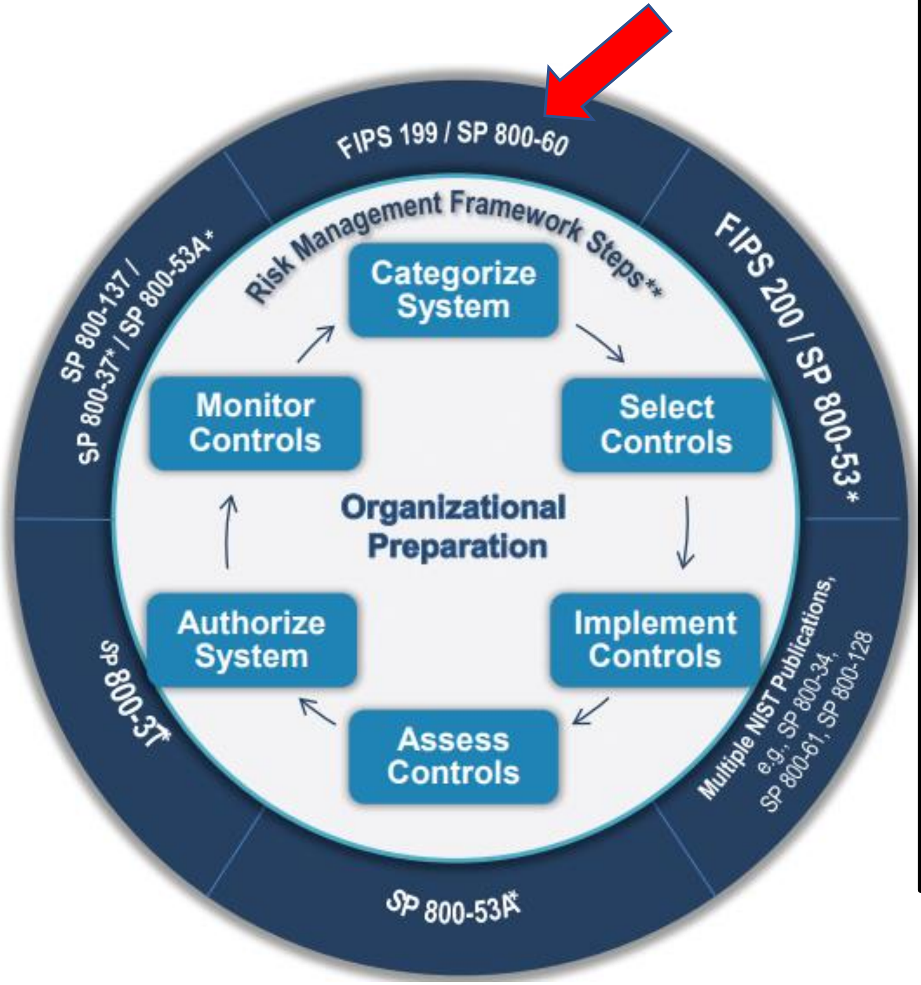
Agenda

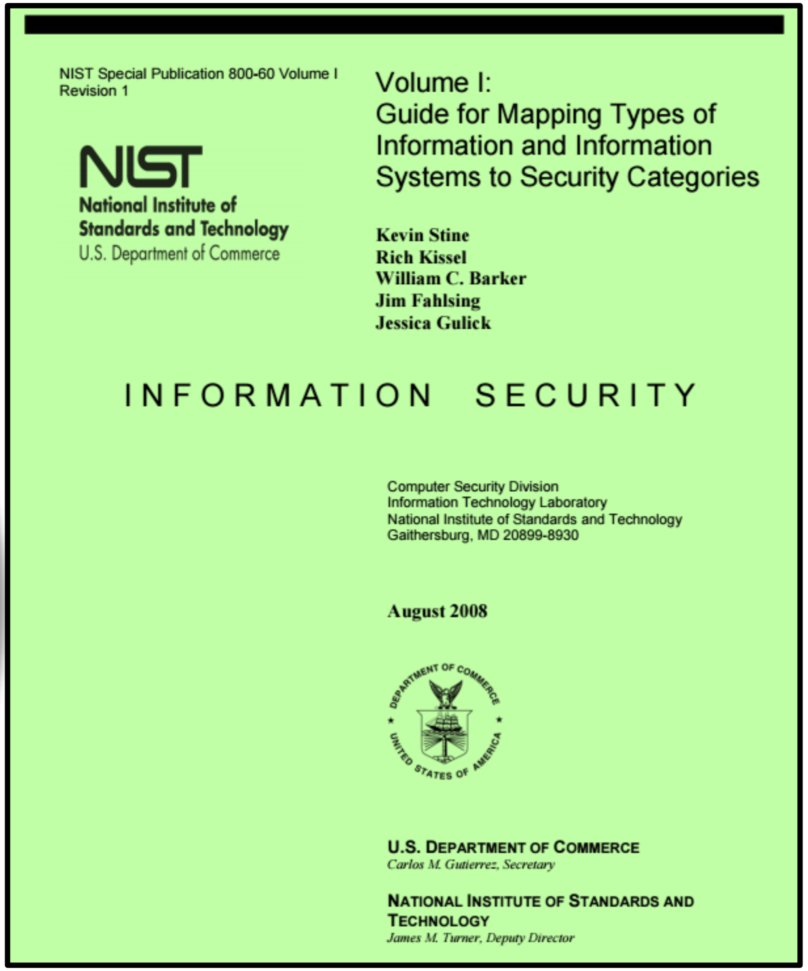
- ✓100 Digits of Pi Quiz
- ✓National Institute of Standards and Technology (NIST)
  - ✓Cybersecurity Framework
  - ✓Risk Management Framework
- Applying the NIST Risk Management Framework
- Milestone 1 Assignment

NIST Risk Management Framework



A guide for provisional security categorization


FIPS 199 / SP 800-60
FIPS 200 / SP 800-53*
Multiple NIST Publications, e.g., SP 800-34, SP 800-61, SP 800-128
SP 800-53A*
SP 800-37*
SP 800-137 / SP 800-37* / SP 800-53A*
Risk Management Framework Steps**
Categorize System
Select Controls
Implement Controls
Assess Controls
Authorize System
Monitor Controls
Organizational Preparation



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

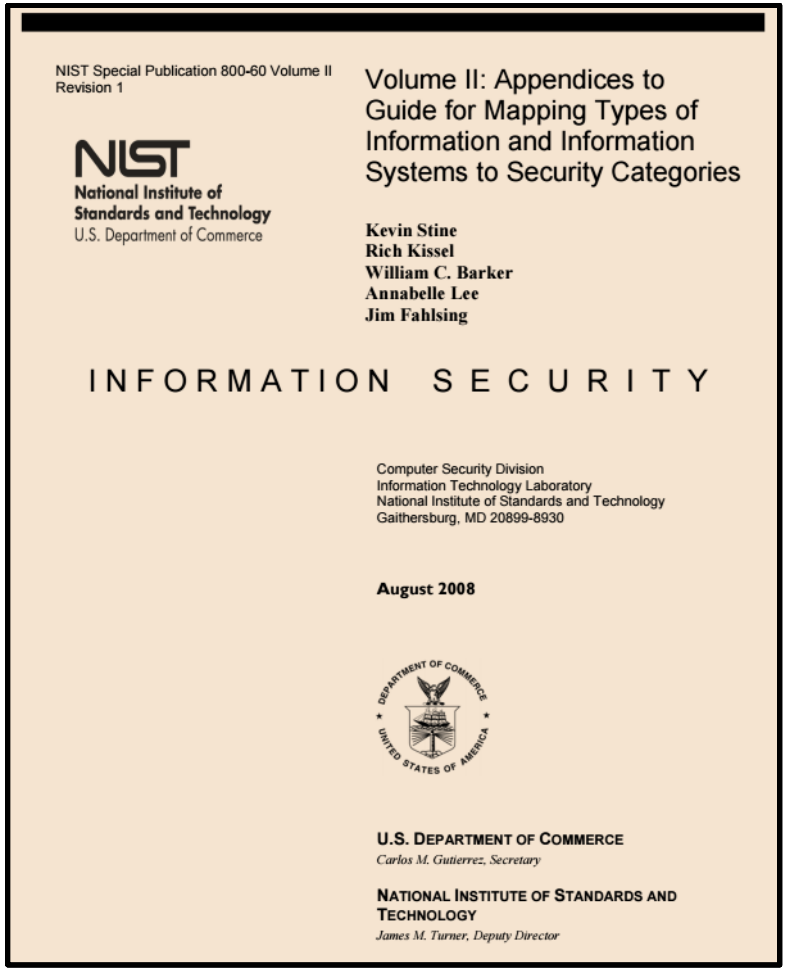
INFORMATION SECURITY

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

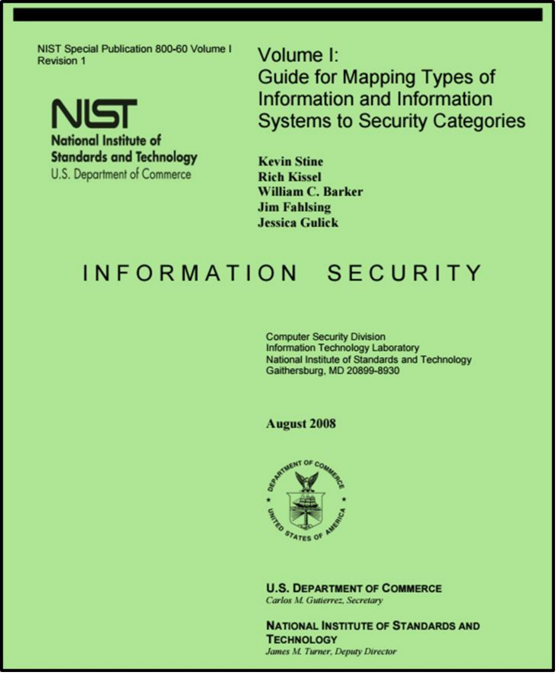
INFORMATION SECURITY

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



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

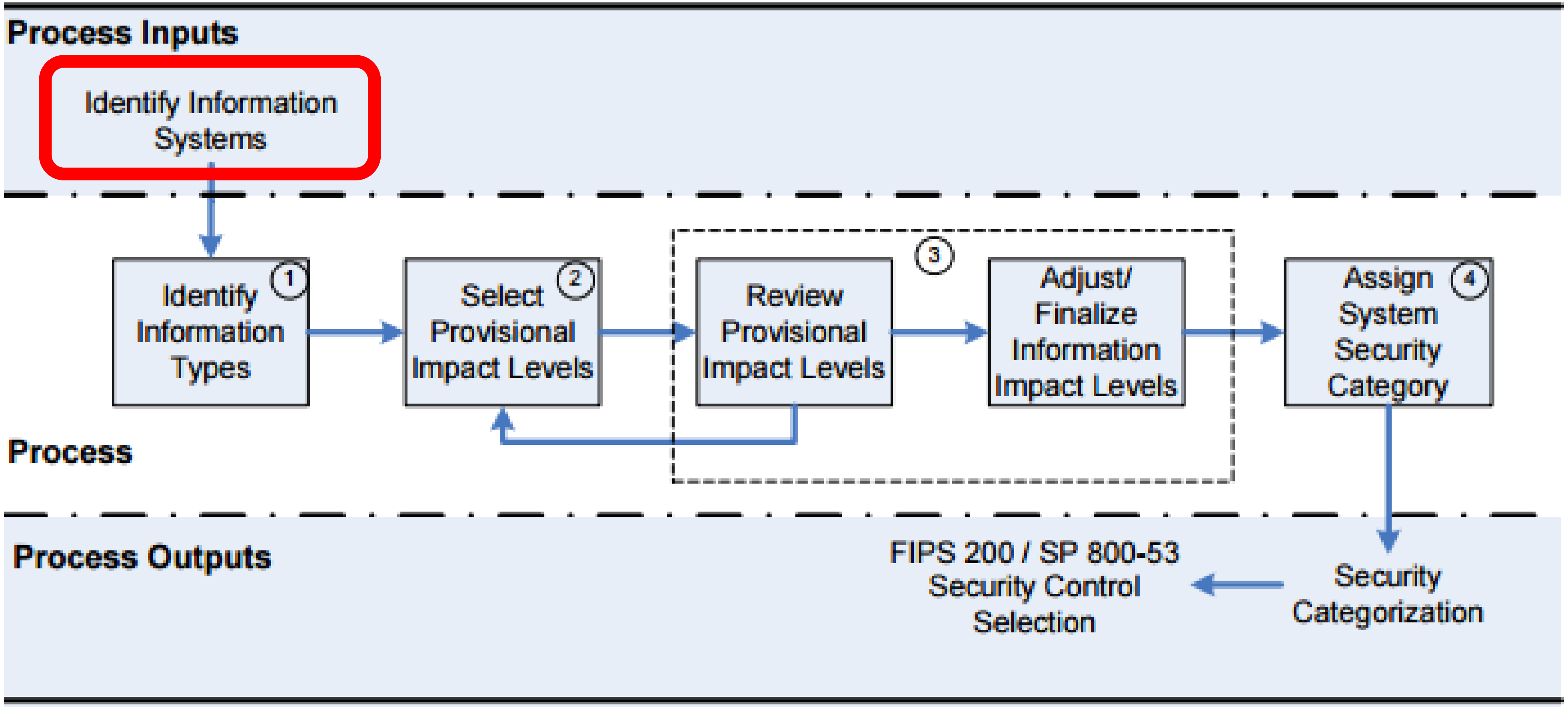
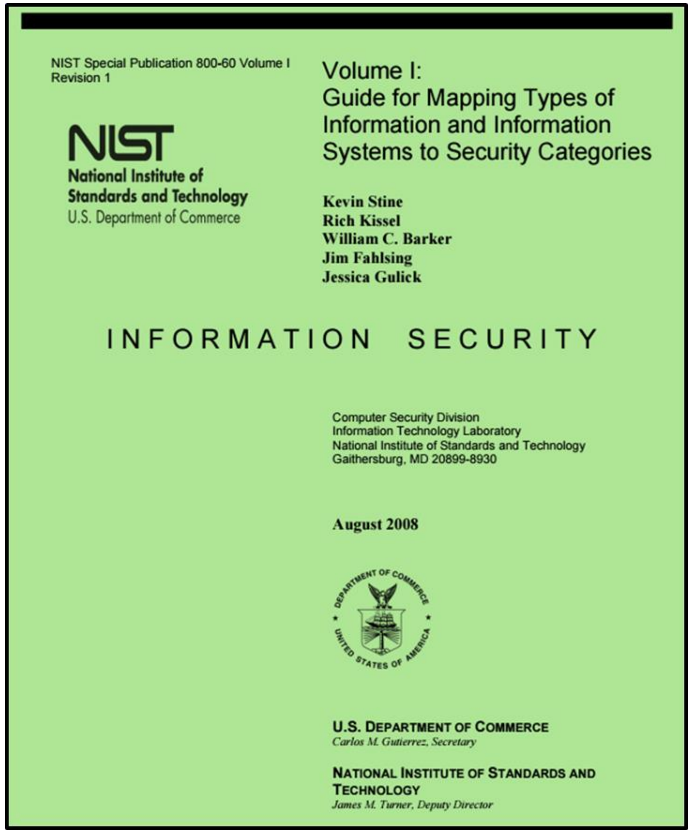

Process Inputs
Identify Information Systems
Identify Information Types 1
Select Provisional Impact Levels 2
3
Review Provisional Impact Levels
Adjust/ Finalize Information Impact Levels
Assign System Security Category 4
Process
Process Outputs
FIPS 200 / SP 800-53 Security Control Selection
Security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

Figure 2: SP 800-60 Security Categorization Process Execution

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 Types

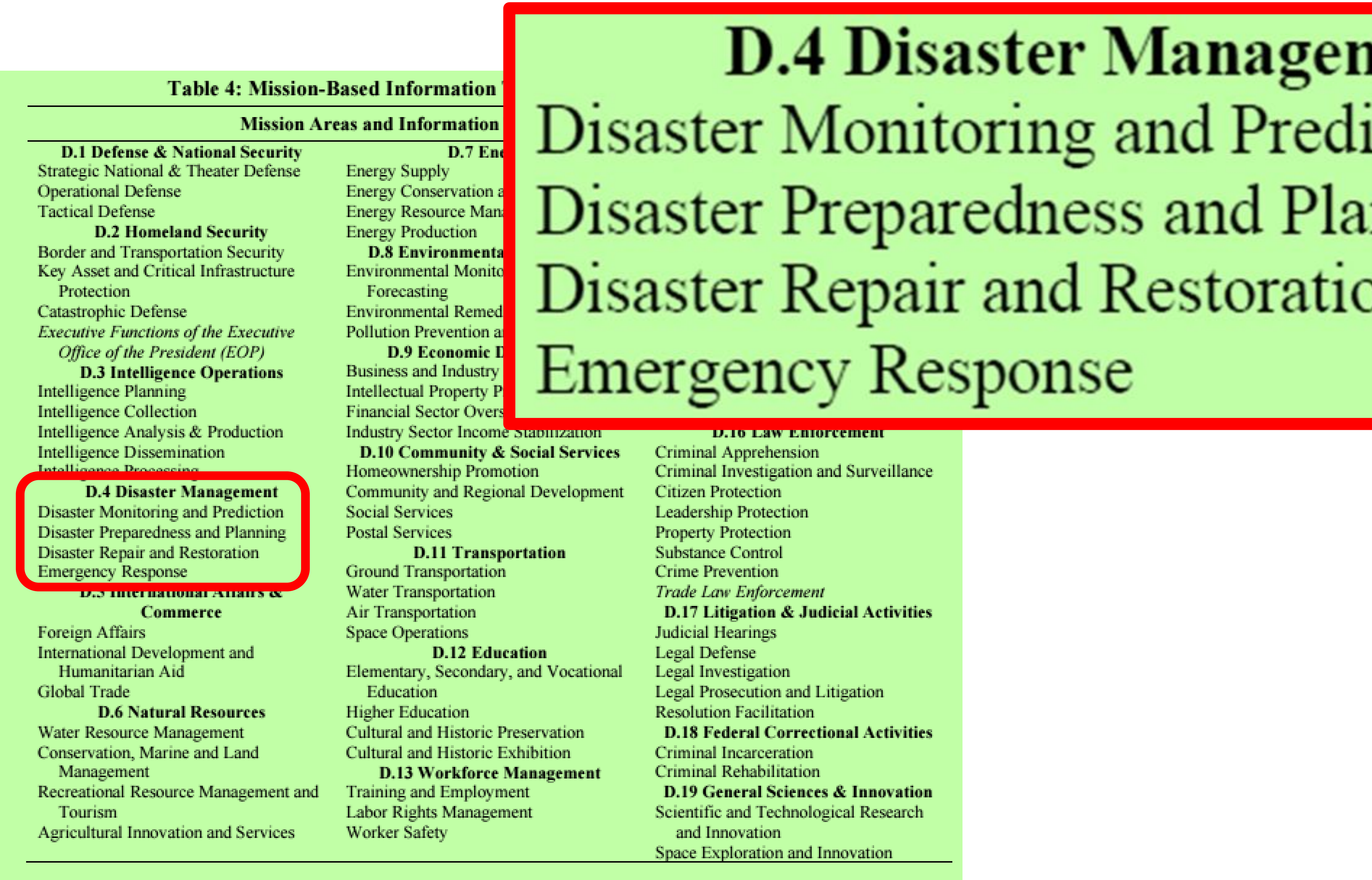


Table 4: Mission-Based Information

Mission Areas and Information

Mode of Delivery]

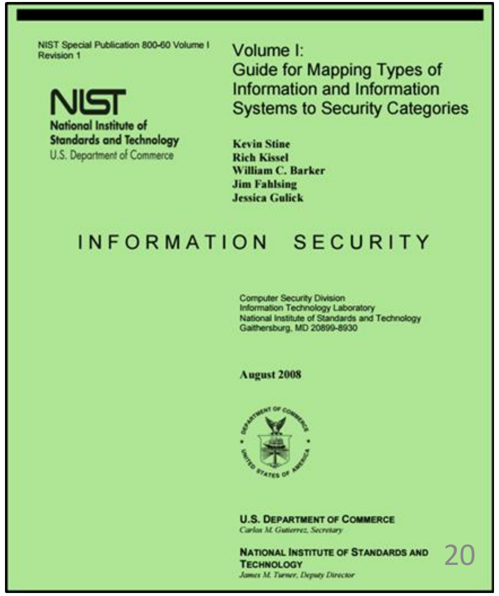
D.1 Defense & National Security
Strategic National & Theater Defense
Operational Defense
Tactical Defense
D.2 Homeland Security
Border and Transportation Security
Key Asset and Critical Infrastructure Protection
Catastrophic Defense
Executive Functions of the Executive Office of the President (EOP)
D.3 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 Ene
Energy Supply
Energy Conservation a
Energy Resource Mana
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

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

D.4 Disaster Management
Disaster Monitoring and Prediction
Disaster Preparedness and Planning
Disaster Repair and Restoration
Emergency Response



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

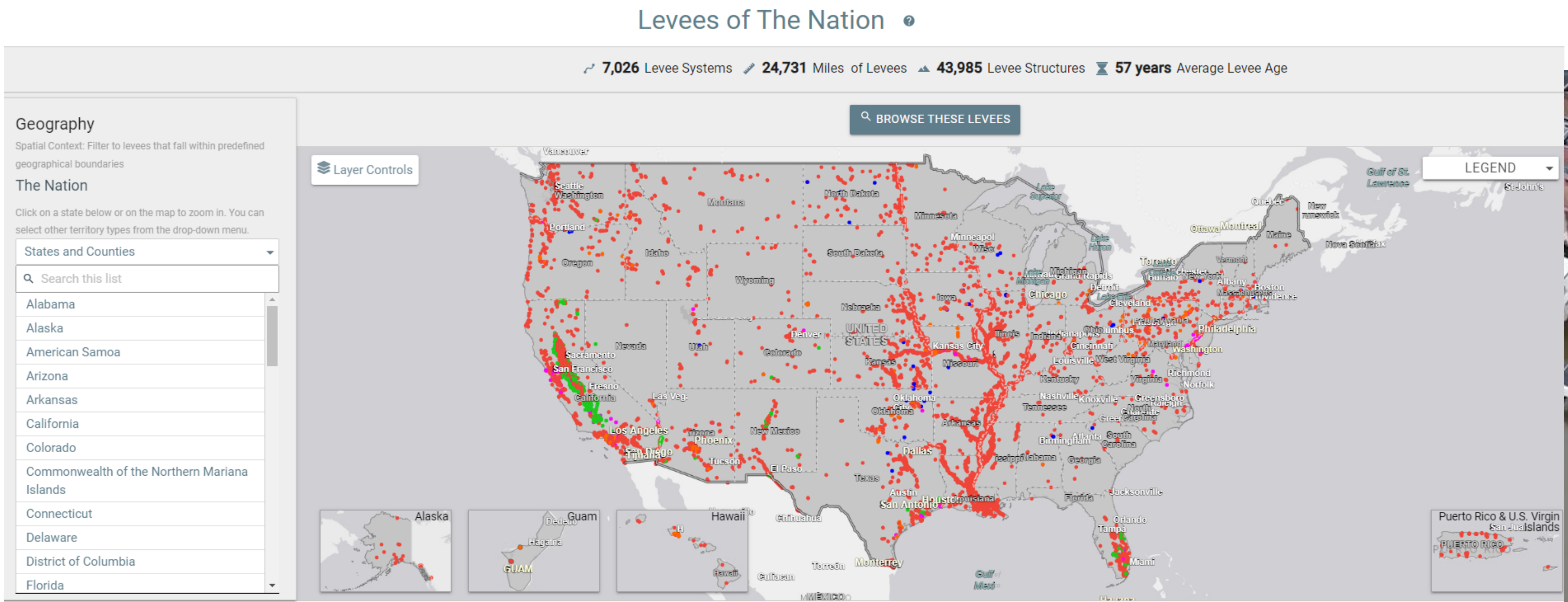
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

August 2008

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

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

Disaster Management Information System Example



Levees of The Nation

7,026 Levee Systems 24,731 Miles of Levees 43,985 Levee Structures 57 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.

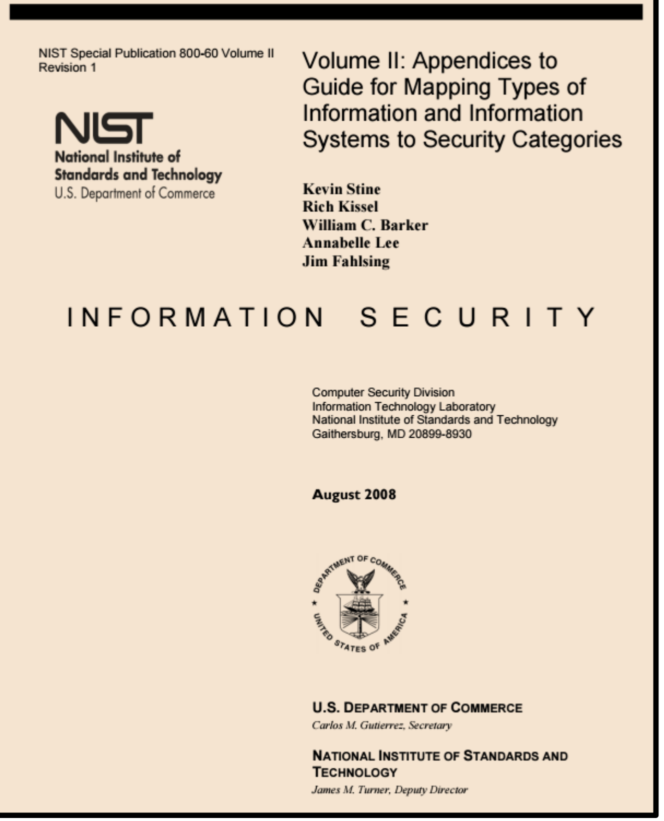
States and Counties

Search this list

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

National Levee Database

2. Select Provisional Impact Levels for the identified information system



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

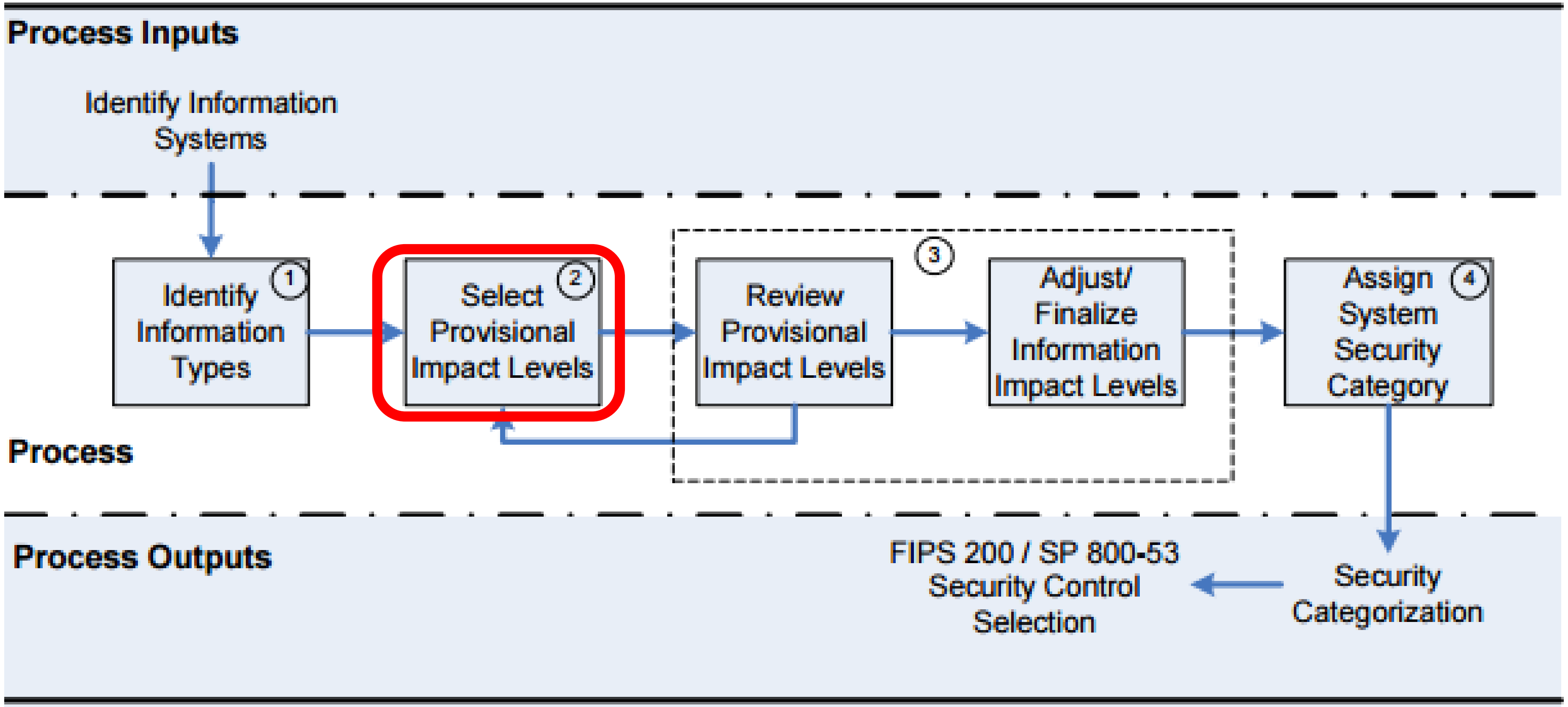
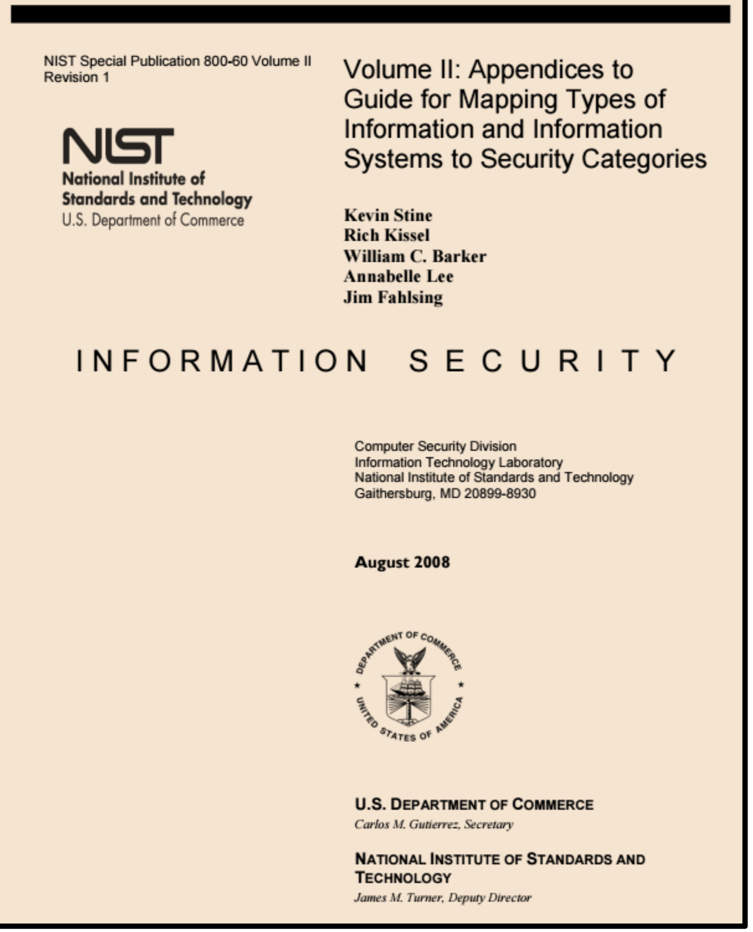

Process Inputs
Identify Information Systems
Identify Information Types 1
Select Provisional Impact Levels 2
3
Review Provisional Impact Levels
Adjust/ Finalize Information Impact Levels
Assign System Security Category 4
Process
Process Outputs
FIPS 200 / SP 800-53 Security Control Selection
Security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

Figure 2: SP 800-60 Security Categorization Process Execution

Disaster Management Information Types



NIST Special Publication 800-60 Volume II
Revision 1

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

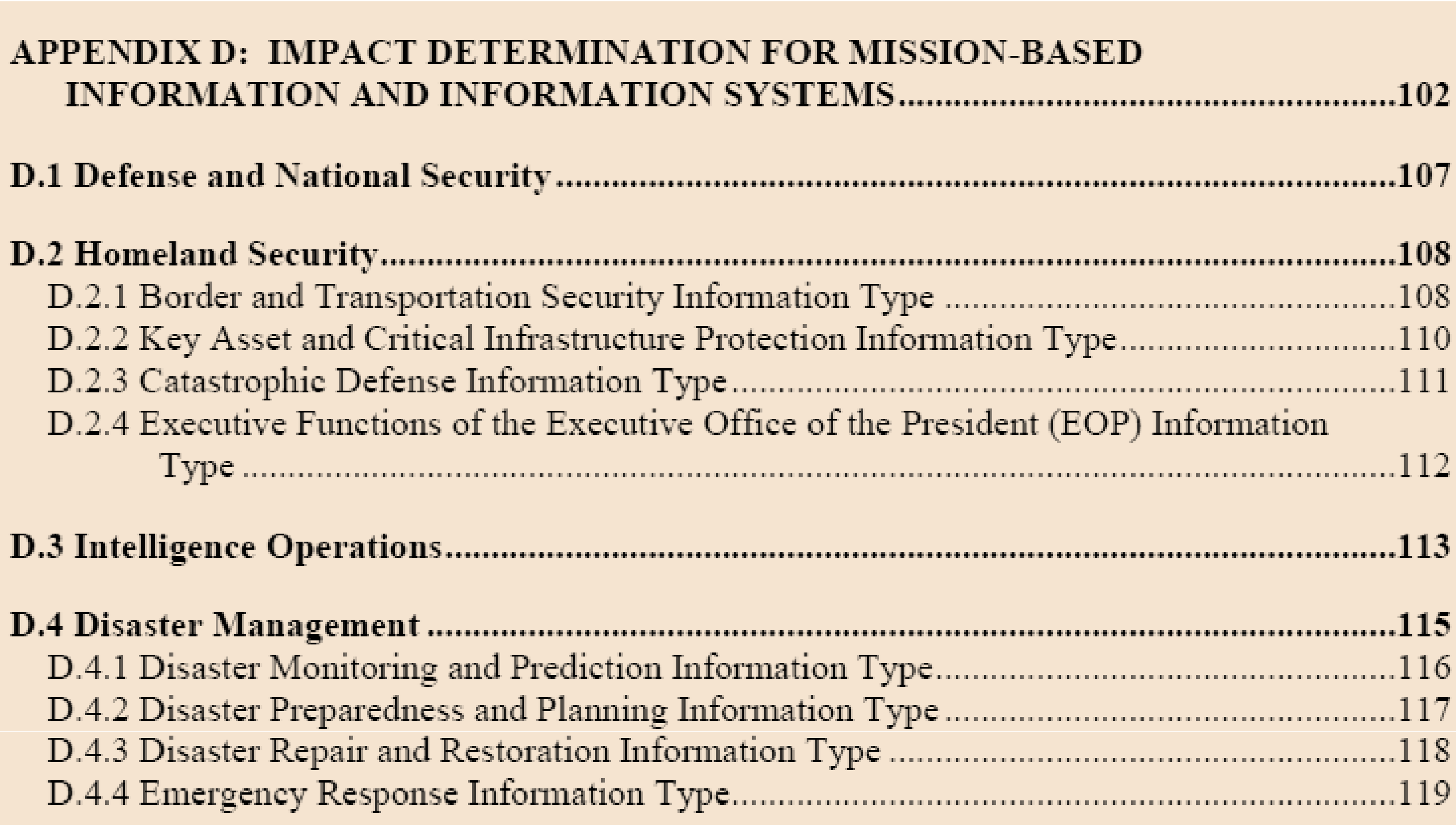
INFORMATION SECURITY

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

August 2008

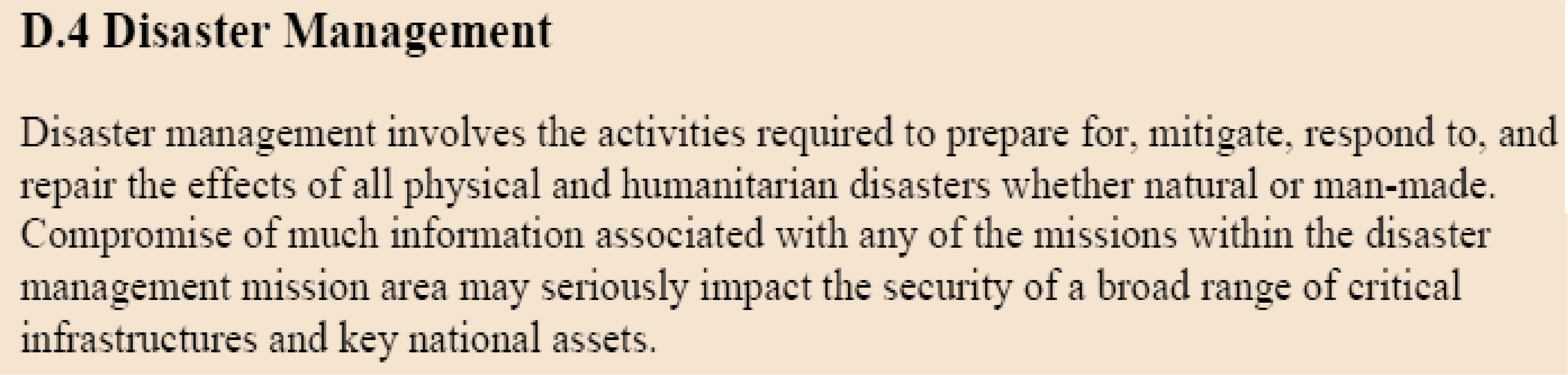
U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

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



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

Disaster Management Information Impact

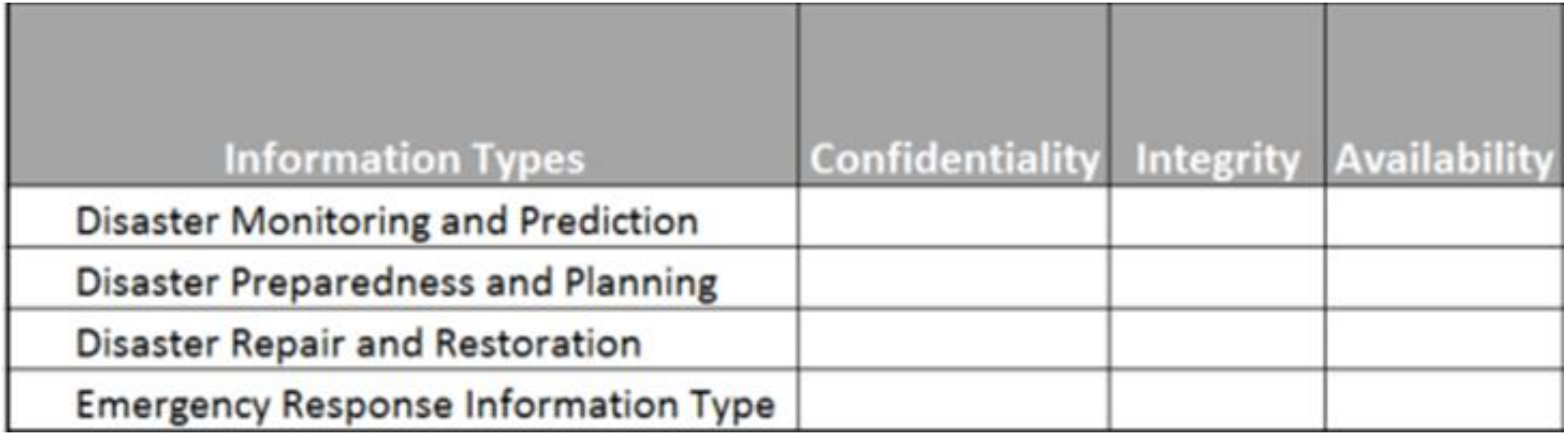


D.4 Disaster Management

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.

Exercise

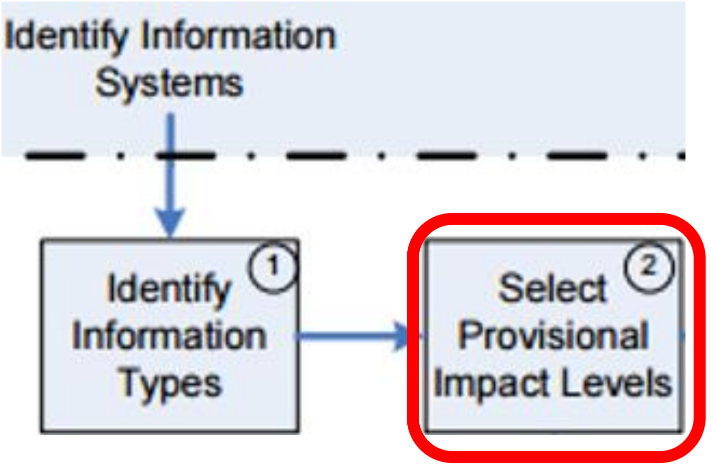
- *Open up an Excel spreadsheet, and organize it in the manner illustrated below*

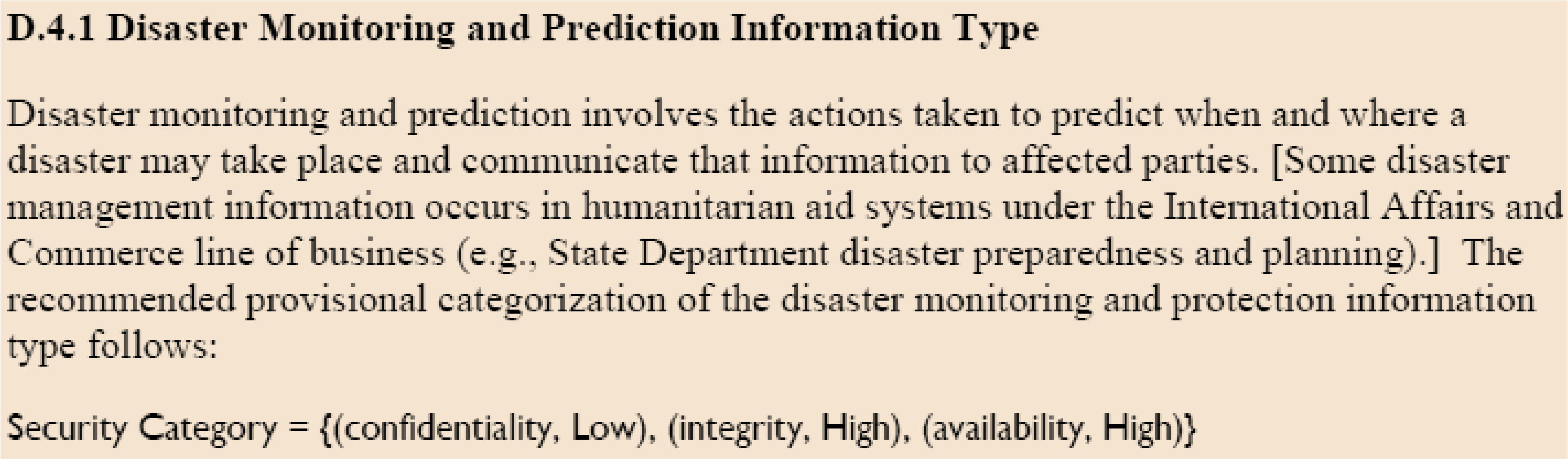


Information Types	Confidentiality	Integrity	Availability
Disaster Monitoring and Prediction			
Disaster Preparedness and Planning			
Disaster Repair and Restoration			
Emergency Response Information Type			

- *Using [NIST SP 800-60 V.2 R1](#) determine the Impact Levels for the Disaster Information Types*

Disaster Management Information Types

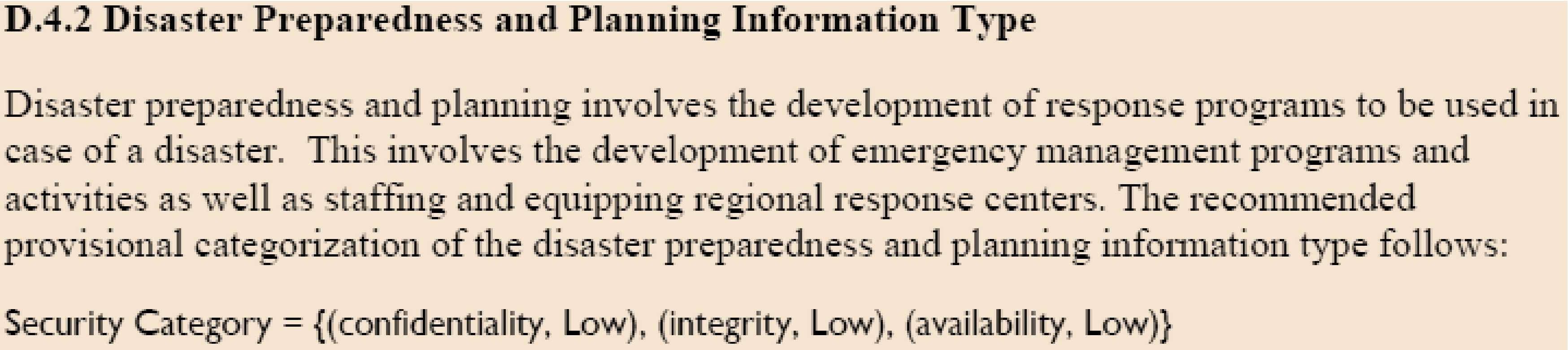

Identify Information Systems
Identify Information Types
1
Select Provisional Impact Levels
2



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:

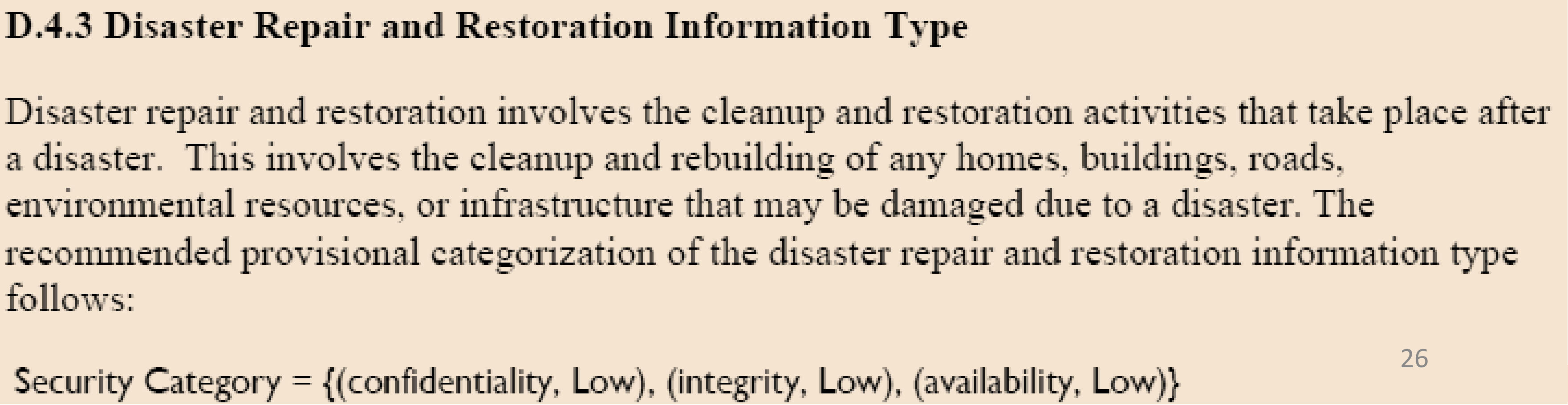
Security Category = {(confidentiality, Low), (integrity, High), (availability, High)}



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)}

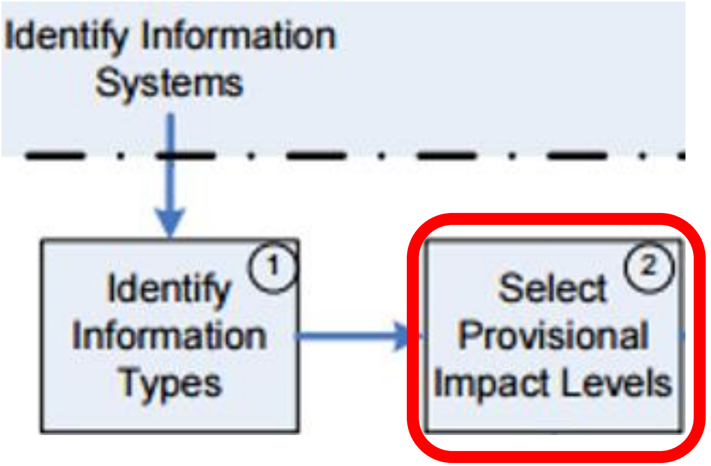


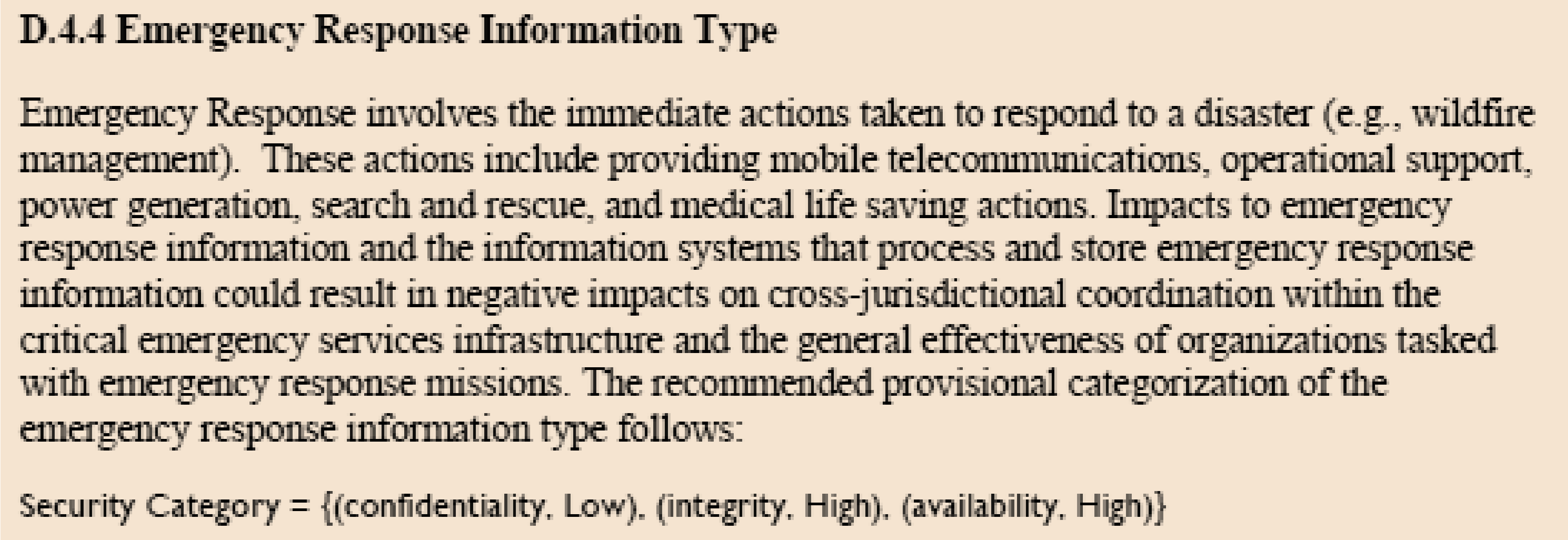
D.4.3 Disaster Repair and Restoration Information Type

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



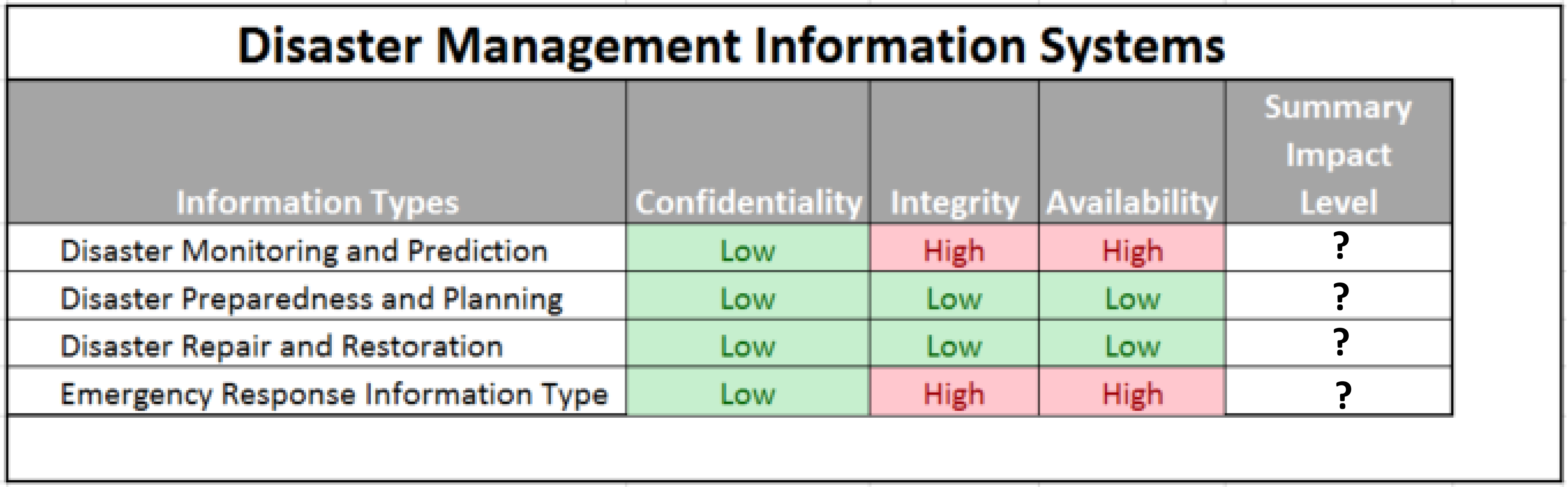
D.4.4 Emergency Response Information Type

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)}

Exercise

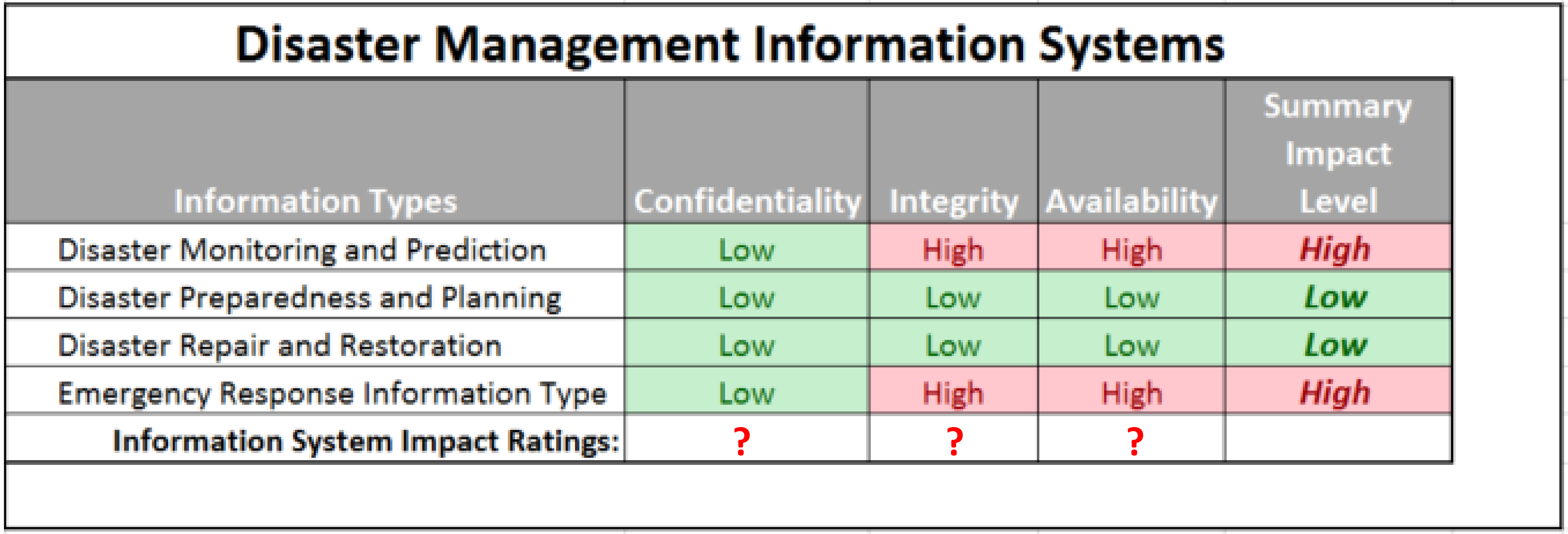
- *Determine the Summary Impact Levels for the Disaster Information Types*



Disaster Management Information Systems

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

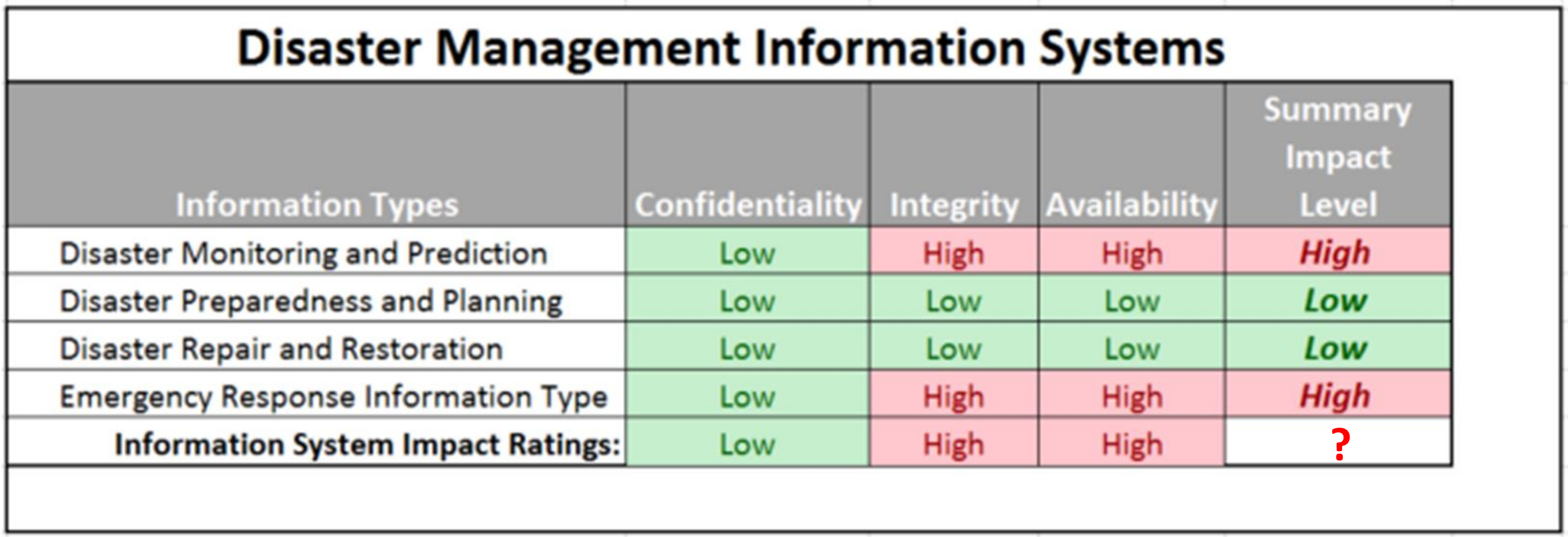
Determine the Overall Impact Levels for the Disaster Information Types



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:	**?**	**?**	**?**	

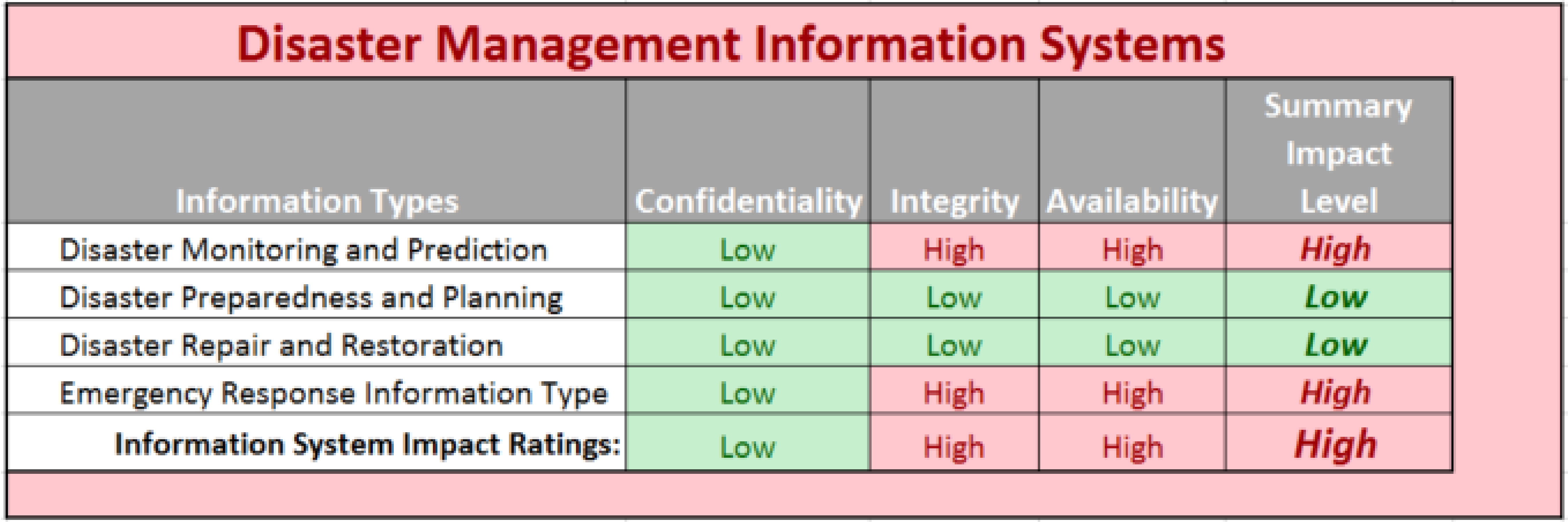
Determine the overall security categorization of a Disaster Information System



Disaster Management Information Systems

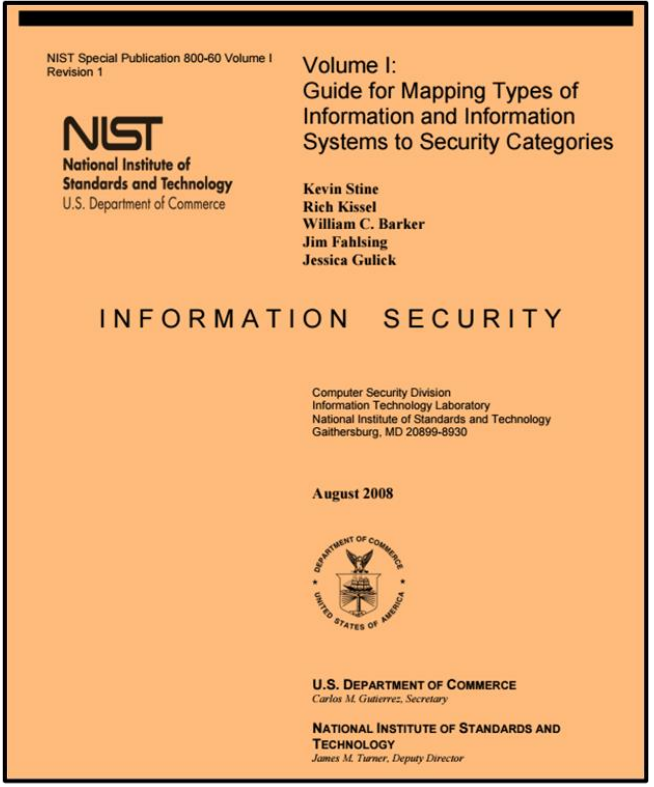
Information Types	Confidentiality	Integrity	Availability	Summary Impact Level
Disaster Monitoring and Prediction	Low	High	High	***High***
Disaster Preparedness and Planning	Low	Low	Low	***Low***
Disaster Repair and Restoration	Low	Low	Low	***Low***
Emergency Response Information Type	Low	High	High	***High***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

Determine the overall security categorization of a Disaster Information System



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 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

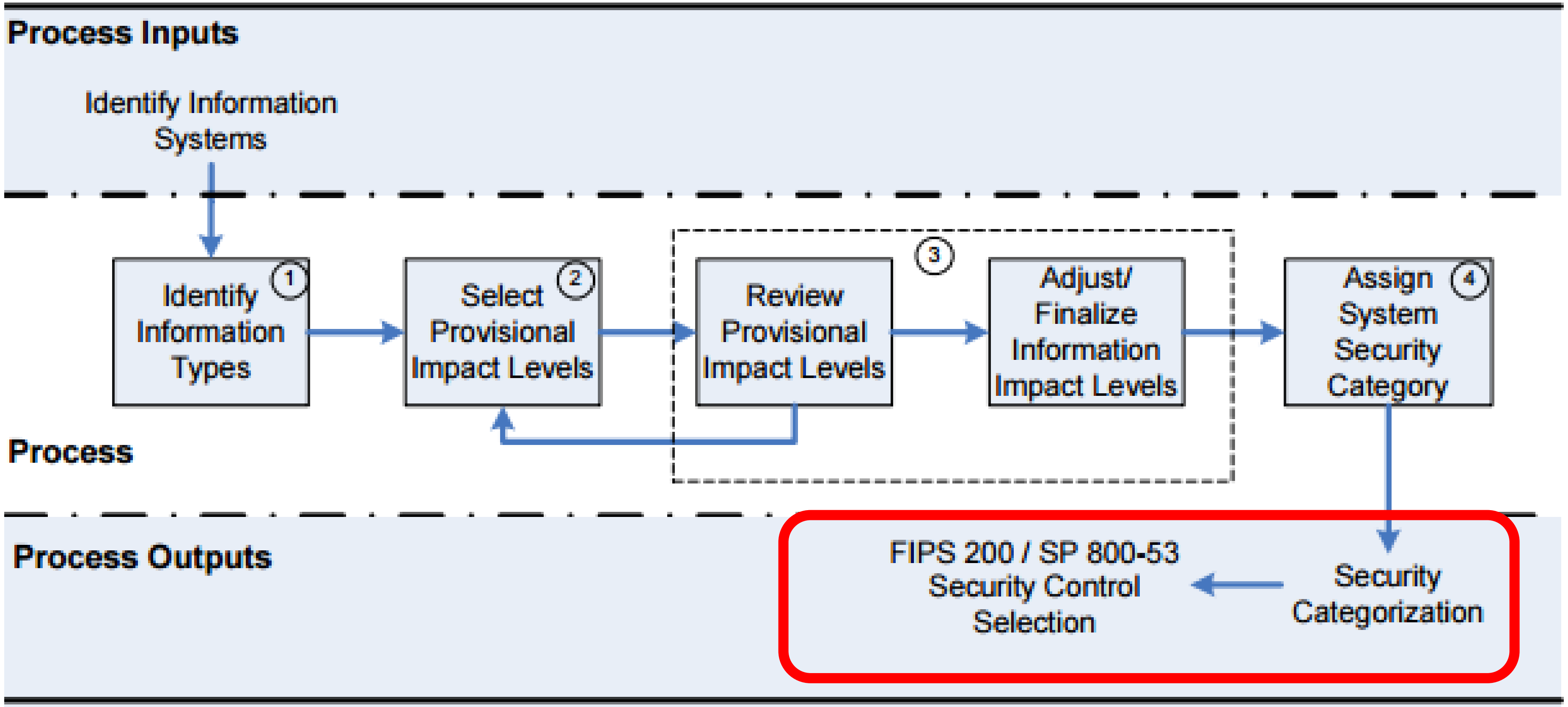
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

August 2008

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

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

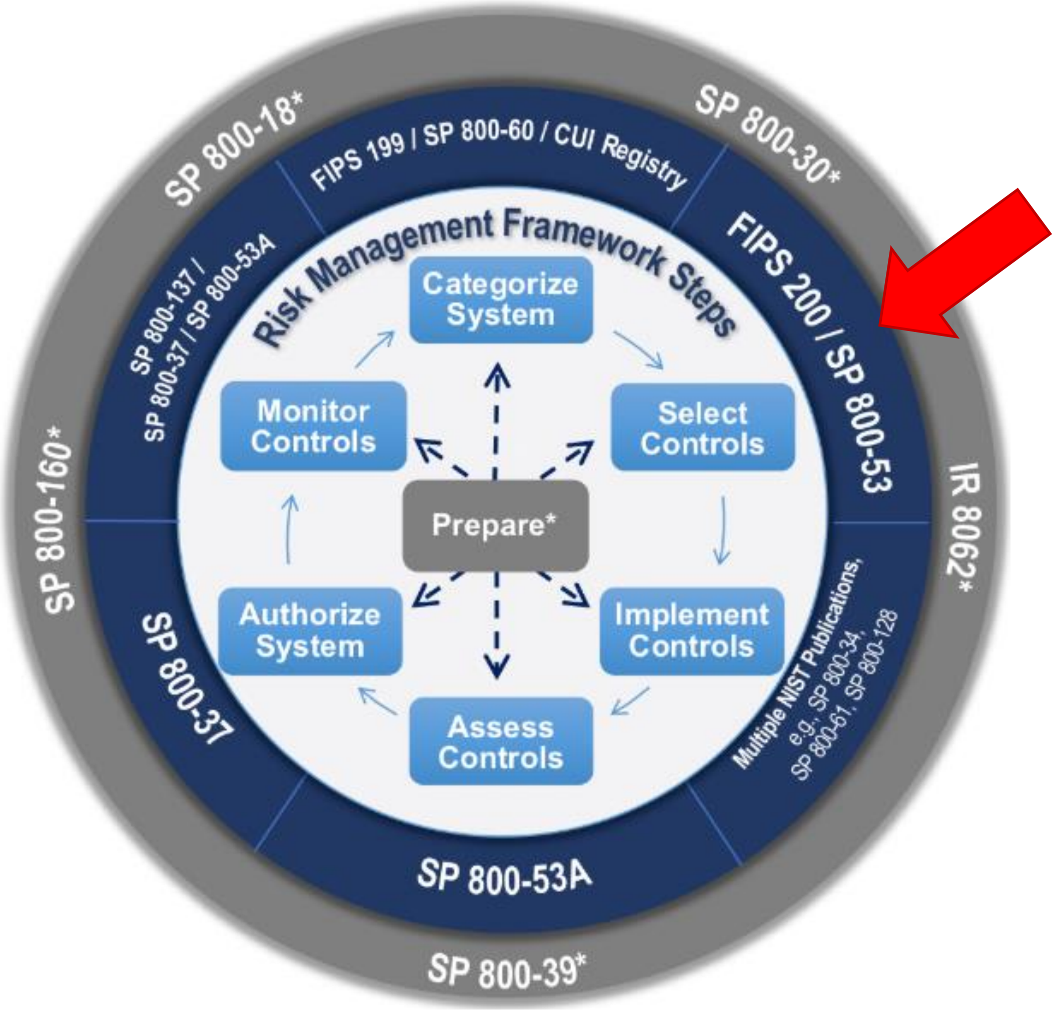
Once categorized, select security control baseline for the information system

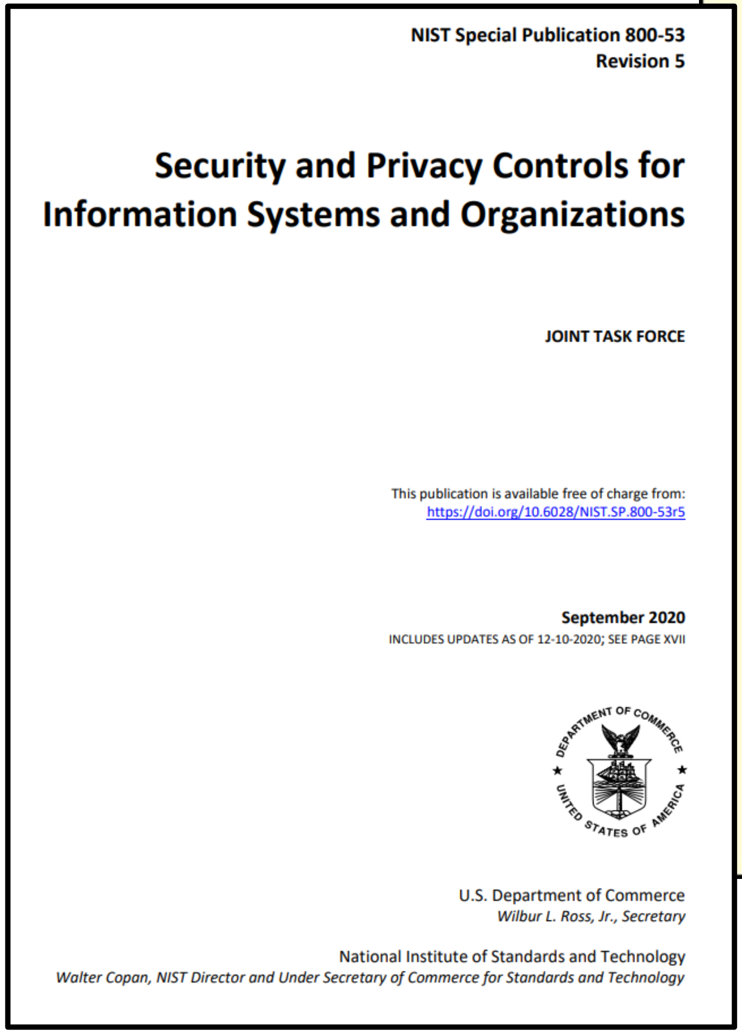


Process Inputs
Identify Information Systems
Identify Information Types 1
Select Provisional Impact Levels 2
3
Review Provisional Impact Levels
Adjust/ Finalize Information Impact Levels
Assign System Security Category 4
Process
Process Outputs
FIPS 200 / SP 800-53 Security Control Selection
Security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

Figure 2: SP 800-60 Security Categorization Process Execution

Selecting cybersecurity risk controls





NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

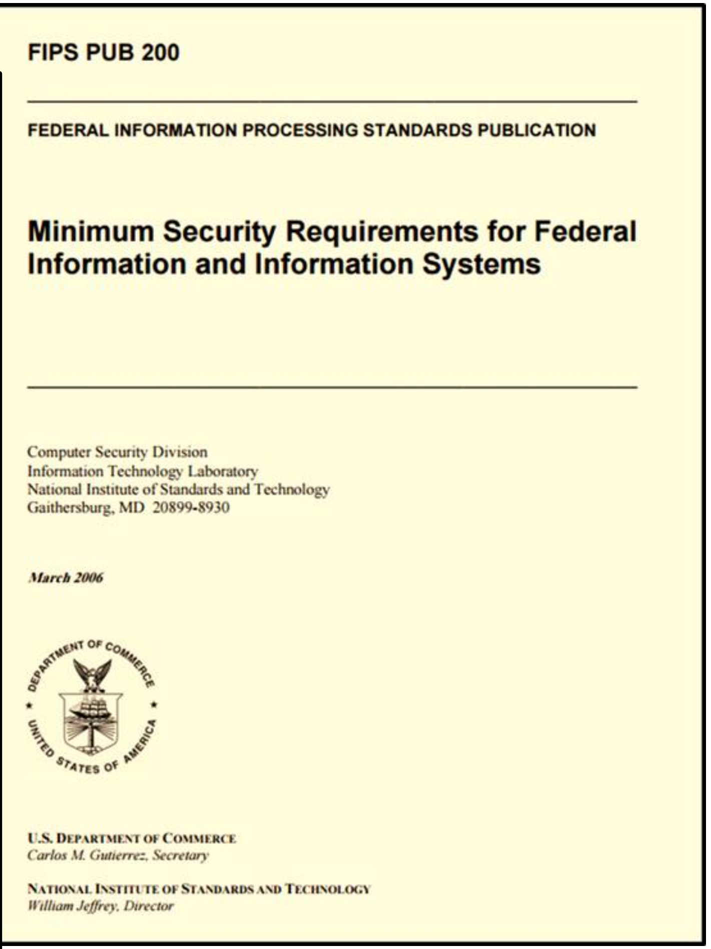
JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5

September 2020
INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XVII

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology



FIPS PUB 200

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Minimum Security Requirements for Federal Information and Information Systems

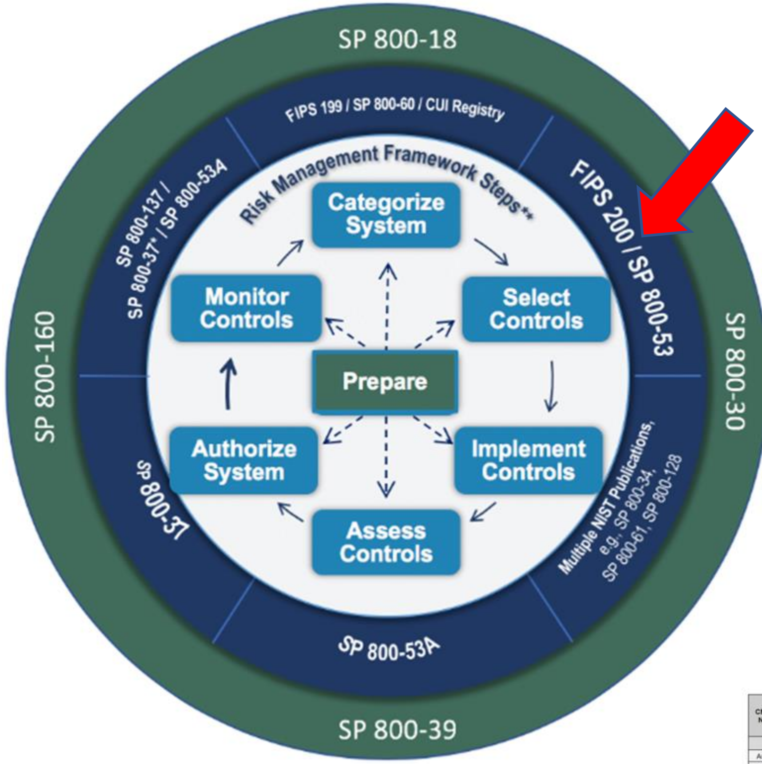
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

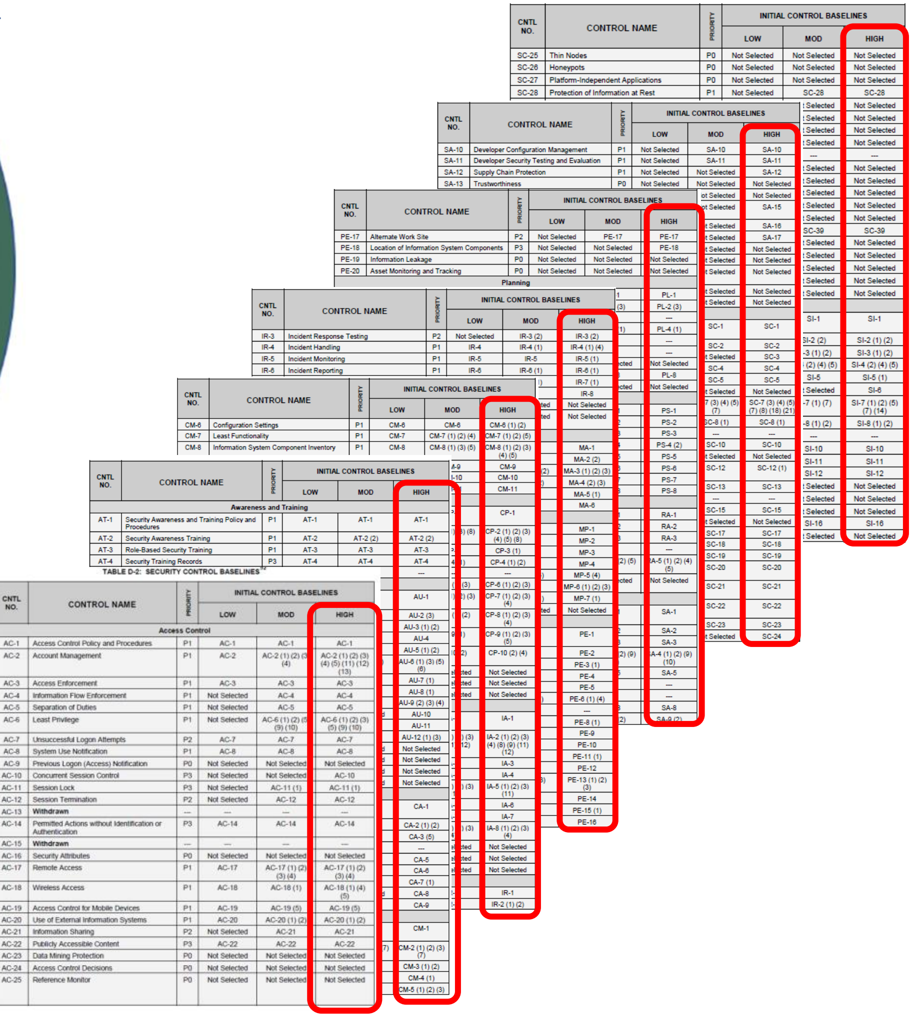
March 2006

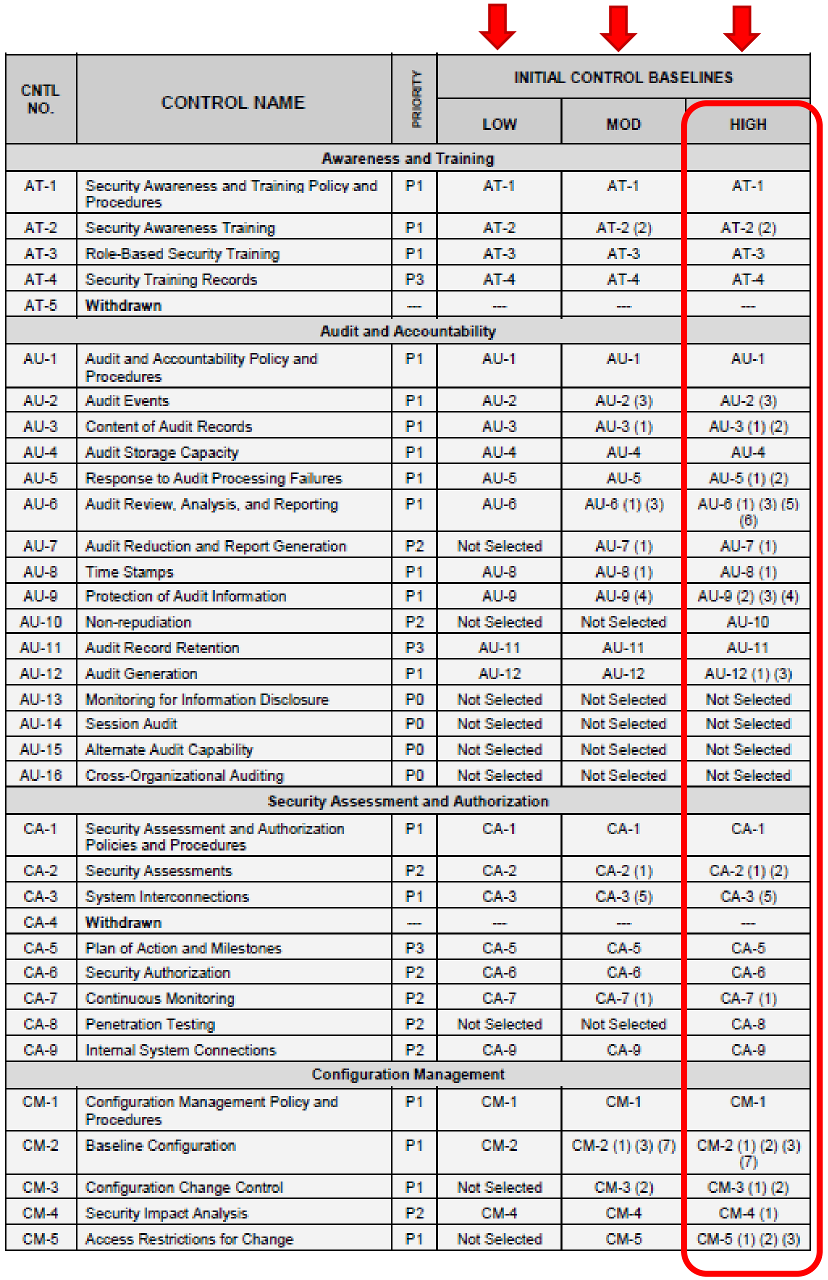
U.S. DEPARTMENT OF COMMERCE
Carlos M. Gutierrez, Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
William Jeffrey, Director

FIPS 199 categorization is used to select among 3 impact-based baselines of security controls







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)

Agenda

- ✓National Institute of Standards and Technology (NIST)
  - ✓Cybersecurity Framework
  - ✓Risk Management Framework
- ✓Applying the NIST Risk Management Framework
- Milestone 1 Assignment
- Prepare for next time to take 100 Digits of Pi Quiz

Milestone 1 – Risk Assessment Report

Milestone 1 Assignment is found in Canvas

Your assignment is to apply the NIST Risk Management Framework and create a risk assessment report for managers of a (fictitious) company that owns and depends on financial information contained in a financial management system

Financial management involves the aggregate set of accounting practices and procedures that allow for the accurate and effective handling of all a business' revenues, funding, and expenditures. A financial management information system supports the following business functions and associated datasets:

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

Your risk assessment will be based on:

1. Security objectives and potential impacts defined in Federal Information Processing Standard 199: "Standards for Security Categorization of Federal Information and Information Systems"
2. Methodology for assigning impact levels to information and information system types described in NIST Special Publication 800-60 Volume I
3. Provisional security categorizations assigned to the financial management information types by NIST Special Publication 800-60 Volume II
4. Determination of an overall security categorization for the financial management information system based on the provisional security categorization of the information types (from 3 above)

What are the Teams ?

Name	Email Address	Team
Ajlani, Zane	tug91318@temple.edu	1
Leinheiser, Edward C	tuh29416@temple.edu	1
Pelna, Matthew A	tug42990@temple.edu	1
Wu, Duke	tuj76216@temple.edu	1
Albertini, Alexander John	tuj64717@temple.edu	2
Lung, Tomson	tug73395@temple.edu	2
Peralta, Loymi	tug26945@temple.edu	2
Yeremian, Paze	tul49918@temple.edu	2
Beasley, Pierre J	tuj05033@temple.edu	3
McGoldrick, Michael James	tug65827@temple.edu	3
Pester, Ben Dov	tuk43388@temple.edu	3
Gentile, Nicholas Jacob	tuj62245@temple.edu	4
McGowan, Brad	tuj66655@temple.edu	4
Phan, James	tug65082@temple.edu	4
Iverson, John	tug80260@temple.edu	5
Morita, Dan	tul43873@temple.edu	5
Pobirsky, Tyler	tug98822@temple.edu	5
Kennedy, Patrick	tui12065@temple.edu	6
Nguyen, Lan	tuj52949@temple.edu	6
Shockley, Jeremy C	tuh38512@temple.edu	6

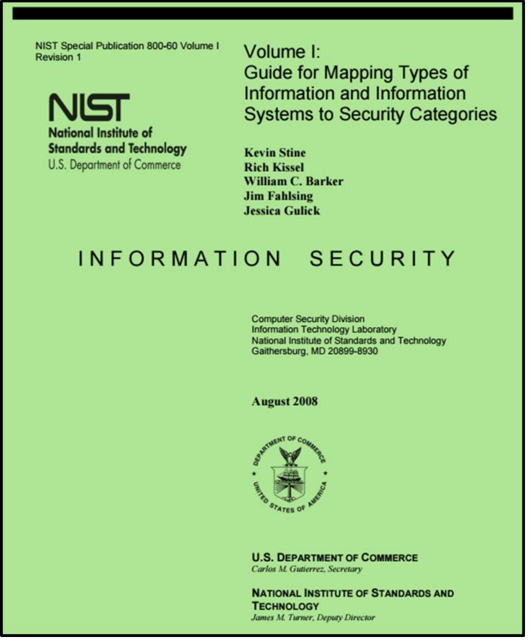
Name	Email Address	Team
Ajlani, Zane	tug91318@temple.edu	
Albertini, Alexander John	tuj64717@temple.edu	
Beasley, Pierre J	tuj05033@temple.edu	
Gentile, Nicholas Jacob	tuj62245@temple.edu	
Iverson, John	tug80260@temple.edu	
Kennedy, Patrick	tui12065@temple.edu	
Leinheiser, Edward C	tuh29416@temple.edu	
Lung, Tomson	tug73395@temple.edu	
McGoldrick, Michael James	tug65827@temple.edu	
McGowan, Brad	tuj66655@temple.edu	
Morita, Dan	tul43873@temple.edu	
Nguyen, Lan	tuj52949@temple.edu	
Pelna, Matthew A	tug42990@temple.edu	
Peralta, Loymi	tug26945@temple.edu	
Pester, Ben Dov	tuk43388@temple.edu	
Phan, James	tug65082@temple.edu	
Pobirsky, Tyler	tug98822@temple.edu	
Shockley, Jeremy C	tuh38512@temple.edu	
Wu, Duke	tuj76216@temple.edu	
Yeremian, Paze	tul49918@temple.edu	

How should you proceed in getting started with Milestone 1 ?

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

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

2 Broad Types of Information and 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

1. Mission-based Information & Information Systems

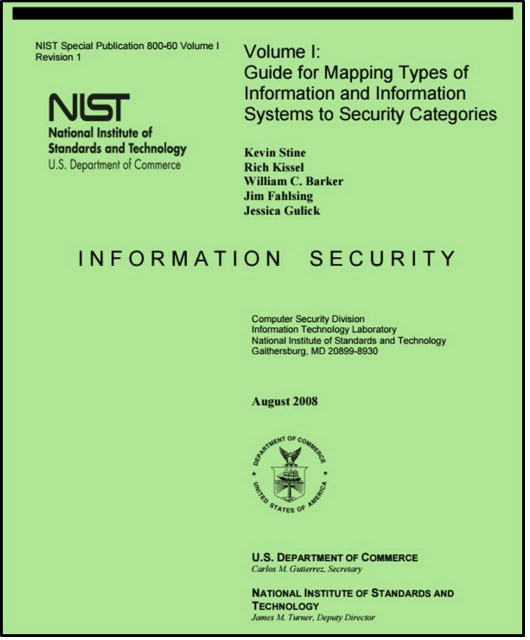
2. **Management and Support Information & Information Systems**

    i. **Services Delivery Support 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

2 Broad Types of Information and 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

1. Mission-based Information & Information Systems

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

    i. **Services Delivery Support Functions**

    ii. **Government Resource Management Functions**

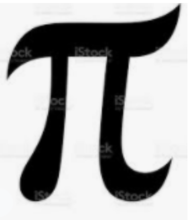
Government Resource Management Functions & Information Types

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

Agenda

- ✓National Institute of Standards and Technology (NIST)
  - ✓Cybersecurity Framework
  - ✓Risk Management Framework
- ✓Applying the NIST Risk Management Framework
- ✓Milestone 1 Assignment
- Prepare for next time to take 100 Digits of Pi Quiz

Next Week’s Quiz



At the start of next class, I will give you five minutes to write out the first 100 digits of pi, from memory, on a sheet of paper

- When time is up, you will show the paper to me
- I will not make you clear your desk, but you will need to close your laptop and put your phone face down on the table or away in your bag or pocket
- I do not expect you to actually memorize the digits of pi—**I want you to cheat**.
- How you choose to cheat is entirely up to you. However, I will observe you in Zoom via your camera. If you are caught cheating, you will fail the quiz. Collaborative cheating is also allowed, but everyone involved will fail the quiz if caught.
- The class will vote on the most creative and effective cheating technique.
- The objective of the exercise is to learn how an adversary thinks and operates by deliberately loosening traditional academic rules and tapping personal creativity. To avoid any misunderstanding, this exception to the traditional ban on cheating only applies to this quiz and not to other graded assignments in the course. Cheating outside of this quiz will not be tolerated.”

Goal: Help you develop a Security Mindset

Agenda

- ✓National Institute of Standards and Technology (NIST)
    - ✓Cybersecurity Framework
    - ✓Risk Management Framework
- ✓Applying the NIST Risk Management Framework
- ✓Milestone 1 Assignment
- ✓Prepare for next time to take 100 Digits of Pi Quiz