



---



# FITSI Federal Body of Knowledge Guide



An Overview of the  
Federal Body of  
Knowledge (FBK) for  
the Federal IT  
Security Professional  
(FITSP) Certification  
Program

Version 2.1

Published 5/30/2019



---

This page is left intentionally blank

---

# TABLE OF CONTENTS

1. EXECUTIVE OVERVIEW .....	4
2. FEDERAL BODY OF KNOWLEDGE OVERVIEW.....	5
3. HOW FITSP USES THE FEDERAL BODY OF KNOWLEDGE .....	6
4. FBK BREAKDOWN .....	7
DOMAINS.....	7
<i>Domain 1 – NIST Special Publications</i> .....	7
<i>Domain 2 - NIST Federal Information Processing Standards</i> .....	9
<i>Domain 3 - NIST Control Families</i> .....	10
<i>Domain 4 - Government Laws and Regulations</i> .....	10
<i>Domain 5 - NIST Risk Management Framework (formerly C&amp;A)</i> .....	15
<i>Domain 6 - NIST Interagency Reports</i> .....	16
IT SECURITY TOPIC AREAS.....	17
<i>Topic Area 1 – Access Control</i> .....	17
<i>Topic Area 2 – Audit and Accountability</i> .....	17
<i>Topic Area 3 – Awareness and Training</i> .....	18
<i>Topic Area 4 – Configuration Management</i> .....	18
<i>Topic Area 5 – Contingency Planning</i> .....	19
<i>Topic Area 6 – Identification and Authentication</i> .....	19
<i>Topic Area 7 – Incident Response</i> .....	20
<i>Topic Area 8 – Maintenance</i> .....	20
<i>Topic Area 9 – Media Protection</i> .....	21
<i>Topic Area 10 – Personnel Security</i> .....	21
<i>Topic Area 11 – Physical and Environmental Protection</i> .....	21
<i>Topic Area 12 – Planning</i> .....	22
<i>Topic Area 13 – Program Management</i> .....	22
<i>Topic Area 14 – Risk Assessment</i> .....	23
<i>Topic Area 15 – Security Assessments and Authorization</i> .....	24
<i>Topic Area 16 – System and Communication Protection</i> .....	24
<i>Topic Area 17 – System and Information Integrity</i> .....	25
<i>Topic Area 18 – System and Services Acquisition</i> .....	25
5. APPENDIX A – RESCINDED PUBLICATIONS .....	27
<i>Domain 1 – NIST Special Publications</i> .....	27
<i>Domain 4 - Government Laws and Regulations</i> .....	27

---

## 1. Executive Overview

The Federal Body of Knowledge (FBK) is a library of federal statutes, regulations, standards, and guidelines that federal workforce security professionals are required to use in protecting and defending systems owned by or operated on behalf of the federal government. Provided by the Federal IT Security Institute (FITSI), the purpose of this document is to help provide interested parties with an understanding of what constitutes the FBK. This document can be used for general knowledge or by Federal IT Security Professional (FITSP) candidates to help augment their study in pursuit of one of the four FITSP certifications (Manager, Designer, Operator, Auditor).

This guide is updated periodically and is meant to provide a high-level description of the body of knowledge that forms the basis of the exams.

This document is available free of charge at the following FITSI website: <http://www.fitsi.org/documents>. It may be forwarded to professional colleagues but must be kept in its original form.

**Important note: This document includes an overview of the FBK that establishes the boundary of knowledge that cuts across all four FITSP certifications. Candidates are not expected to have read and understood all of the publications listed.**

---

## 2. Federal Body of Knowledge Overview

The FBK is broken down into six domains and 18 IT security topic areas.

### Domains

1. Domain 1 – NIST Special Publications
2. Domain 2 – NIST Federal Information Processing Standards (FIPS)
3. Domain 3 – NIST Control Families
4. Domain 4 – Governmental Laws and Regulations
5. Domain 5 – NIST Risk Management Framework
6. Domain 6 – NIST Interagency Reports

### IT Security Topic Areas\*

1. Access Control
2. Audit and Accountability
3. Awareness and Training
4. Configuration Management
5. Contingency Planning
6. Identification and Authentication
7. Incident Response
8. Maintenance
9. Media Protection
10. Personnel Security
11. Physical and Environmental Protection
12. Planning
13. Program Management
14. Risk Assessment
15. Security Assessment and Authorization
16. System and Communications Protection
17. System and Information Integrity
18. System and Services Acquisition

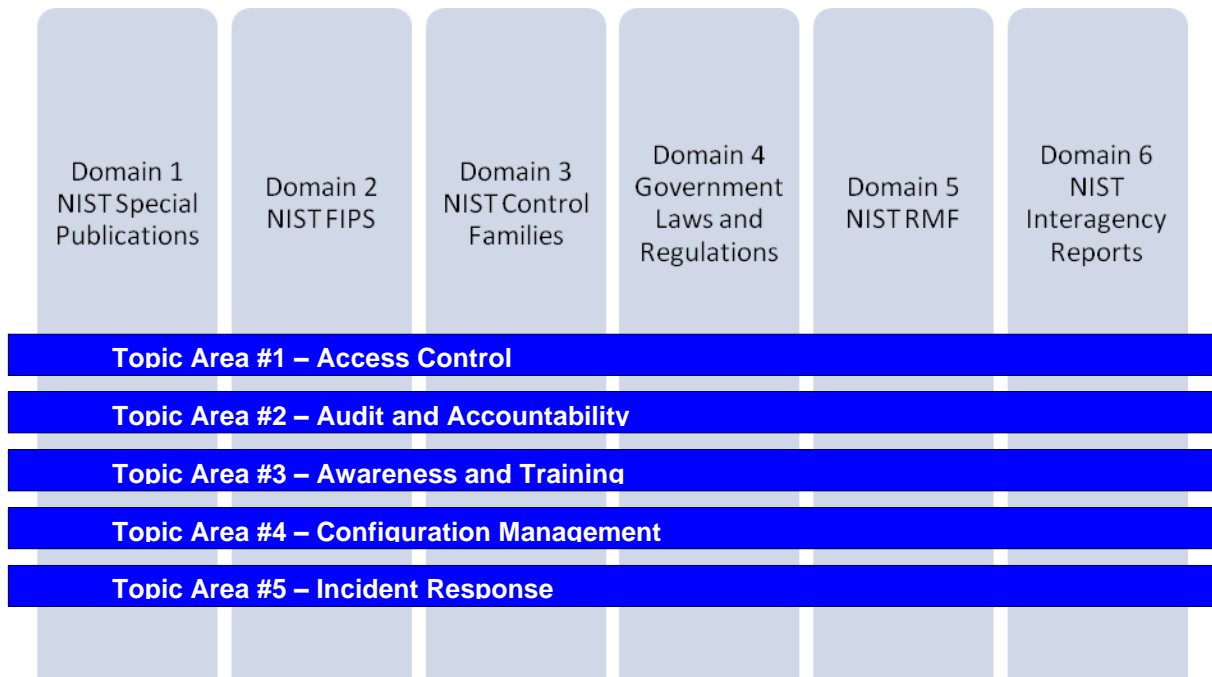
\* Seventeen of the 18 IT Security topic areas are derived directly from the minimum control requirements defined in Federal Information Processing Standard 200 (FIPS 200), one is from NIST SP 800-53 (Appendix G, Program Management).

---

### 3. How FITSP uses the Federal Body of Knowledge

Domains are the boundaries of knowledge that apply to the federal government. The IT Security topic areas include themes and skills that IT security professionals are expected to understand. *The FITSP role-based exams for Manager, Designer, Operator, and Auditor include questions that cover the intersection between the six domains and the 18 IT security topic areas (see illustration below).*

The interwoven nature of the domains and topic areas are below. Only five out of the 18 topic areas are present for illustration purposes.



---

## 4. FBK Breakdown

The purpose of this section is to provide the reader with a broad overview of the domains and topic areas. Because the exam focuses on federal statutes, regulations, standards, and guidelines, this guide provides a breakdown for each FITSP domain and topic area.

This document provides the reader with a reference on what constitutes the boundary of the FBK.

### ***Domains***

#### **Domain 1 – NIST Special Publications**

NIST Special Publications are written to provide guidance and best practices to federal agencies on how to protect the agency's missions, business functions, and environment of operation. These publications are downloadable for free at the following website:

<http://csrc.nist.gov>.

1. 800-12 Rev1 -An Introduction to Computer Security: The NIST Handbook
2. 800-15 - MISPC Minimum Interoperability Specification for PKI Components, Version 1
3. 800-16 - Information Technology Security Training Requirements: A Role- and Performance-Based Model
4. 800-18 Rev 1 - Guide for Developing Security Plans for Federal Information Systems
5. 8800-25 - Federal Agency Use of Public Key Technology for Digital Signatures and Authentication
6. 800-28 Version 2 - Guidelines on Active Content and Mobile Code
7. 800- 30 Rev 1 - Guide for Conducting Risk Assessments
8. 800-32 - Introduction to Public Key Technology and the Federal PKI Infrastructure
9. 800-34 Rev. 1 - Contingency Planning Guide for Federal Information Systems
10. 800-35 - Guide to Information Technology Security Services
11. 800-37 Rev 1 - Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
12. 800-37 Rev 2 - Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
13. 800-39 Managing Information Security Risk: Organization, Mission, and Information System View
14. 800-40 Rev. 3 - Guide to Enterprise Patch Management Technologies
15. 800-41Rev 1 - Guidelines on Firewalls and Firewall Policy
16. 800-44 Version 2 - Guidelines on Securing Public Web Servers
17. 800-45 Version 2 - Guidelines on Electronic Mail Security
18. 800-46 Rev. 2 - Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security
19. 800-47 - Security Guide for Interconnecting Information Technology Systems
20. 800-48 Rev 1 - Guide to Securing Legacy IEEE 802.11 Wireless Networks
21. 800-49 - Federal S/MIME V3 Client Profile
22. 800-50 Building an Information Technology Security Awareness and Training Program
23. 800-51 Rev. 1 - Guide to Using Vulnerability Naming Schemes
24. 800-52 Rev. 1 - Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
25. 800-53 Rev4 - Security and Privacy Controls for Federal Information Systems and Organizations
26. 800-53A Rev. 4 - Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans

- 
27. 800-55 Rev 1 - Performance Measurement Guide for Information Security
  28. 800-57 Part 1 Rev. 4 - Recommendation for Key Management, Part 1: General
  29. 800-57 Part 2 - Recommendation for Key Management, Part 2: Best Practices for Key Management Organization
  30. 800-57 Part 3 Rev. 1 - Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance
  31. 800-59 - Guideline for Identifying an Information System as a National Security System
  32. 800-60 Rev 1 - Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) - Volume 1: Guide Volume 2: Appendices
  33. 800-61 Rev. 2 - Computer Security Incident Handling Guide
  34. 800-63-3 - Digital Identity Guidelines
  35. 800-63A - Digital Identity Guidelines: Enrollment and Identity Proofing
  36. 800-63B - Digital Identity Guidelines: Authentication and Lifecycle Management
  37. 800-63C - Digital Identity Guidelines: Federation and Assertions
  38. 800-64 Rev 2 – Security Considerations in the System Development Life Cycle
  39. 800-66 Rev 1 - An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
  40. 800-70 Rev. 4 - National Checklist Program for IT Products: Guidelines for Checklist Users and Developers
  41. 800-77 - Guide to IPsec VPNs
  42. 800-78-4 - Cryptographic Algorithms and Key Sizes for Personal Identity Verification
  43. 800-79-2 - Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)
  44. 800-81-2 - Secure Domain Name System (DNS) Deployment Guide
  45. 800-82 Rev. 2 - Guide to Industrial Control Systems (ICS) Security
  46. 800-83 Rev. 1 - Guide to Malware Incident Prevention and Handling for Desktops and Laptops
  47. 800-84 - Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
  48. 800-85A4 PIV Card Application and Middleware Interface Test Guidelines (SP 800-73-4 Compliance)
  49. 800-85B PIV Data Model Test Guidelines
  50. 800-86 - Guide to Integrating Forensic Techniques into Incident Response
  51. 800-87 Rev 2 - Codes for Identification of Federal and Federally-Assisted Organizations
  52. 800-88 Rev. 1 - Guidelines for Media Sanitization
  53. 800-89 Recommendation for Obtaining Assurances for Digital Signature Applications
  54. 800-92 - Guide to Computer Security Log Management
  55. 800-94 - Guide to Intrusion Detection and Prevention Systems (IDPS)
  56. 800-95 - Guide to Secure Web Services
  57. 800-96 - PIV Card to Reader Interoperability Guidelines
  58. 800-97 - Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i
  59. 800-98 - Guidelines for Securing Radio Frequency Identification (RFID) Systems
  60. 800-100 - Information Security Handbook: A Guide for Managers
  61. 800-101 Rev. 1 - Guidelines on Mobile Device Forensics
  62. 800-102 - Recommendation for Digital Signature Timeliness
  63. 800-106 Randomized Hashing for Digital Signatures
  64. 800-107 Rev 1 - Recommendation for Applications Using Approved Hash Algorithms
  65. 800-111 - Guide to Storage Encryption Technologies for End User Devices
  66. 800-113 - Guide to SSL VPNs
  67. 800-114 Rev. 1 - User's Guide to Telework and Bring Your Own Device (BYOD) Security
  68. 800-115 - Technical Guide to Information Security Testing and Assessment
  69. 800-116 Rev 1 Guidelines for the Use of PIV Credentials in Facility Access
  70. 800-117 - Guide to Adopting and Using the Security Content Automation Protocol (SCAP) Version 1.0
  71. 800-119 - Guidelines for the Secure Deployment of IPv6
  72. 800-121 Rev. 2 - Guide to Bluetooth Security
  73. 800-122 - Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
  74. 800-123 - Guide to General Server Security



- 
75. 800-124 Rev. 1 - Guidelines for Managing the Security of Mobile Devices in the Enterprise
  76. 800-125 - Guide to Security for Full Virtualization Technologies
  77. 800-126 Rev. 3 - The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2
  78. 800-126A - SCAP 1.3 Component Specification Version Updates: An Annex to NIST Special Publication 800-126 Revision 3
  79. 800-128 - Guide for Security-Focused Configuration Management of Information Systems
  80. 800-130 A Framework for Designing Cryptographic Key Management Systems
  81. 800-133 Recommendation for Cryptographic Key Generation
  82. 800-137 - Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
  83. 800-144 - Guidelines on Security and Privacy in Public Cloud Computing
  84. 800-145 - The NIST Definition of Cloud Computing
  85. 800-146 - Cloud Computing Synopsis and Recommendations
  86. 800-147 - BIOS Protection Guidelines
  87. 800-150 - Guide to Cyber Threat Information Sharing
  88. 800-152 A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS)
  89. 800-153 - Guidelines for Securing Wireless Local Area Networks (WLANs)
  90. 800-157 Guidelines for Derived Personal Identity Verification (PIV) Credentials
  91. 800-160 Volume 1 - Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
  92. 800-161 - Supply Chain Risk Management Practices for Federal Information Systems and Organizations
  93. 800-162 - Guide to Attribute Based Access Control (ABAC) Definition and Considerations
  94. 800-163 Vetting the Security of Mobile Applications
  95. 800-167 - Guide to Application Whitelisting
  96. 800-171 Rev. 1 - Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations
  97. 800-179 Guide to Securing Apple OS X 10.10 Systems for IT Professionals: A NIST Security Configuration Checklist
  98. 800-181 - NICE Cybersecurity Workforce Framework (NCWF): National Initiative for Cybersecurity Education
  99. 800-183 - Networks of 'Things'
  - 100.800-184 - Guide for Cybersecurity Event Recovery
  - 101.800-190 Application Container Security Guide
  - 102.800-192 Verification and Test Methods for Access Control Policies/Models

## Domain 2 - NIST Federal Information Processing Standards

The FBK includes the list of all NIST Federal Information Processing Standards (FIPS). These standards are downloadable at the following website: <http://csrc.nist.gov>.

1. FIPS 202 - SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions
2. FIPS 201-2 - Personal Identity Verification (PIV) of Federal Employees and Contractors
3. FIPS 200 - Minimum Security Requirements for Federal Information and Information Systems
4. FIPS 199 - Standards for Security Categorization of Federal Information and Information Systems
5. FIPS 198-1 - The Keyed-Hash Message Authentication Code
6. FIPS 197 - Advanced Encryption Standard
7. FIPS 186-4 - Digital Signature Standard (DSS)
8. FIPS 180-4 - Secure Hash Standard (SHS)
9. FIPS 140-2 - Security Requirements for Cryptographic Modules

---

## Domain 3 - NIST Control Families

NIST SP 800-53 identifies 18 IT security control families used in the design of federal information systems.

1. Access Control
2. Awareness and Training
3. Audit and Accountability
4. Security Assessment and Authorization
5. Configuration Management
6. Contingency Planning
7. Identification and Authentication
8. Incident Response
9. Maintenance
10. Media Protection
11. Physical and Environmental Protection
12. Planning
13. Personnel Security
14. Risk Assessment
15. System and Services Acquisition
16. System and Communication Protection
17. System and Information Integrity
18. Program Management (organization level)

## Domain 4 - Government Laws and Regulations

Listed below are the Acts of Congress, OMB memos, executive orders and presidential directives that impact federal IT systems. Acts of Congress, executive orders, and presidential directive are available on the Internet. OMB memos and circulars are downloadable from <http://www.whitehouse.gov/omb>.

1. Acts of Congress
  - a) Privacy Act of 1974
    - a. as amended 5 U.S.C. § 552a.
  - b) Paperwork Reduction Act of 1980
    - a. 44 USC § 3501, et. seq.
  - c) Computer Security Act of 1987
    - a. Replaced by FISMA and is no longer in effect
  - d) Chief Financial Officers Act of 1990
  - e) Government Performance and Results Act of 1993
  - f) Paperwork and Elimination Act of 1998
  - g) Government Information Security Reform Act
    - a. Replace by FISMA and is no longer in effect
  - h) Federal Information Security Management Act of 2002
    - a. 44 U.S.C. 3541, et. Seq.
  - i) Health Insurance Portability and Accountability Act
  - j) Clinger-Cohen Act of 1996
  - k) The Health Information Technology for Economic and Clinical Health Act (HITECH) – 2009
  - l) Federal Information Security Modernization Act of 2014
  - m) National Cybersecurity Protection Act of 2014

- 
- n) Cybersecurity Workforce Assessment Act of 2014
  - o) Cybersecurity Enhancement Act of 2014
  - p) Federal Information Technology Acquisition Reform Act
  - q) Cybersecurity Information Sharing Act (CISA)-2015
  - r) Federal Exchange Data Breach Notification Act of 2015
- National Cybersecurity Protection Advancement Act of 2015

## 2. Council of the Inspectors General for Integrity and Efficiency (CIGIE)

- a) IG FISMA Maturity Model Assessment Framework

## 3. DHS Binding Operational Directives

- a) BOD 16-02, Threat to Network Infrastructure Devices
- b) BOD 16-03, 2016 Agency Cybersecurity Reporting Requirements
- c) BOD 17-01 - Removal of Kaspersky-branded Products
- d) BOD 18-01 - Enhance Email and Web Security
- e) BOD 18-02 - Securing High Value Assets
- f) BOD 19-01 - Mitigate DNS Infrastructure Tampering BOD 19-02 - Vulnerability Remediation Requirements for Internet-Accessible Systems

## 4. DHS Federal Information Security Memorandum

- a) FISM 14-01 - Fiscal Year 2014 Metrics for the Federal Information Security Management Act of 2002 and Agency Privacy Management Act and Operational Reporting Instructions
- b) FISM 13-01 FY2013 Reporting Instructions for FISMA and Agency Privacy Management
- c) FISM 12-02 - FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
- d) FISM 12-01 - Protected BIOS for New Procurements of Desktop and Laptop Computers
- e) FISM 11-02 - FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management

## 5. DHS FISMA Documents

- a) FY 2018 CIO FISMA Metrics Effective FY 2018 Quarter 3
- b) FY 2018 IG FISMA Metrics
- c) FY 2018 IG FISMA Metrics Evaluation Guide
- d) FY 2018 SAOP FISMA Metrics
- e) FY 17 SAOP FISMA Metrics
- f) FY17 CIO Annual FISMA Metrics
- g) FY17 IG FISMA Metrics
- h) FY16 CIO Annual FISMA Metrics
- i) FY16 IG FISMA Metrics
- j) FY16 SAOP FISMA Metrics
- k) FY15 CIO Annual FISMA Metrics
- l) FY15 IG FISMA Metrics
- m) FY15 SAOP FISMA Metrics
- n) FY15 CIO Q3 FISMA Metrics
- o) FY15 CIO Q2 FISMA Metrics
- p) FY15 CIO Q1 FISMA Metrics

---

## 6. Executive Orders

- a) EO 13833 - Enhancing the Effectiveness of Agency Chief Information Officers
- b) EO 13718 - Commission on Enhancing National Cybersecurity
- c) EO 13800 - Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
- d) EO 13636 - Improving Critical Infrastructure Cybersecurity
- e) EO 12958 – Classified National Security Information
- f) 36 Code of Federal Regulation Part 1236, Management of Vital Records, revised as of July 1, 2000
- g) 41 Code of Federal Regulations 101.20.103-4, *Occupant Emergency Program*, revised as of July 1, 2000
- h) EO 12472 – Assignment of National Security and Emergency Preparedness Telecommunications Functions
- i) EO 12656 – Assignment of Emergency Preparedness Responsibilities
- j) EO 13231 – Critical Infrastructure Protection in the Information Age

## 7. Federal Audit Standards

- a) Government Audit Standards (Yellow Book)
- b) GAO / PCIE Financial Audit Manual (FAM)
- c) GAO Federal Information Systems Control Audit Manual (FISCAM)

## 8. Federal CIO Council Guidance

- a) Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance Version 2.0

## 9. FedRAMP Program Management Documents

- a) FedRAMP Security Assessment Framework Version 2.4

## 10. Homeland Security Presidential Directives

- a) HSPD-3 – Homeland Security Advisory System
- b) HSPD-5 – Management of Domestic Incidents
- c) HSPD-8 – National Preparedness
- d) HSPD-12 – Policy for a Common Identification Standard for Federal Employees and Contractors
- e) HSPD-20/NSPD-51 – National Continuity Policy
- f) HSPD-24 – Biometrics for Identification and Screening to Enhance National Security

## 11. National Initiative for Cybersecurity Education (NICE)

- a) NICE Framework 2.0

## 12. NIST Cyber Security Framework Documents

- a) Framework for Improving Critical Infrastructure Cybersecurity Version 1.1

---

### 13. OMB Circular

- a) Office of Management and Budget Circular A-11, Preparation, Submission and Execution of the Budget, June 2018
- b) Office of Management and Budget Circular A-123, Management Responsibility for Internal Control, December 2004
- c) Office of Management and Budget Circular A-127-Revised, Financial Management Systems, January 2009
- d) Office of Management and Budget Circular A-130, Managing Information as a Strategic Resource, July 2016

### 14. OMB Memoranda

- 1) M-19-03, Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program
- 2) M-19-02, Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements
- 3) M-18-23 - Shifting From Low-Value to High-Value Work
- 4) M-18-16, Appendix A to OMB Circular No. A-123, Management of Reporting and Data Integrity Risk
- 5) M-18-12, Implementation of the Modernizing Government Technology Act
- 6) M-17-26, Reducing Burden for Federal Agencies by Rescinding and Modifying OMB Memoranda
- 7) M-17-25, Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
- 8) M-17-15, Rescission of Memoranda Relating to Identity Management
- 9) M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information
- 10) M-17-09, Management of Federal High Value Assets
- 11) M-17-06, Policies for Federal Agency Public Websites and Digital Services
- 12) M-16-24, Role and Designation of Senior Agency Officials for Privacy
- 13) M-16-17, OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control
- 14) M-16-15, Federal Cybersecurity Workforce Strategy
- 15) M-16-04, Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government
- 16) M-16-02, Category Management Policy 15-1: Improving the Acquisition and Management of Common Information Technology: Laptops and Desktops
- 17) M-15-14, Management and Oversight of Federal Information Technology
- 18) M-14-16, Guidance on Managing Email
- 19) M-14-04, Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
- 20) M-14-03, Enhancing the Security of Federal Information and Information Systems
- 21) M-13-13, Open Data Policy - Managing Information as an Asset
- 22) M-12-20, FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
- 23) M-11-33, FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
- 24) M-11-29, Chief Information Officer Authorities
- 25) M-11-27, Implementing the Telework Enhancement Act of 2010: Security Guidelines
- 26) M-11-11, Continued Implementation of Homeland Security Presidential Directive (HSPD) 12—Policy for a Common Identification Standard for Federal Employees and Contractors
- 27) M-11-08, Initial Assessments of Safeguarding and Counterintelligence Postures for Classified National Security Information in Automated Systems
- 28) M-11-06, WikiLeaks - Mishandling of Classified Information

- 
- 29) M-11-02, Sharing Data While Protecting Privacy
  - 30) M-10-31, Immediate Review of Information Technology Projects
  - 31) M-10-27, Information Technology Investment Baseline Management Policy
  - 32) M-10-26, Immediate Review of Financial Systems IT Projects
  - 33) M-10-25, Reforming the Federal Government's Efforts to Manage Information Technology Projects
  - 34) M-10-23, Guidance for Agency Use of Third-Party Websites and Applications
  - 35) M-10-10, Federal Agency Coordination on Health Information Technology (HIT)
  - 36) M-09-32 – Update on the Trusted Internet Connections Initiative
  - 37) M-09-02 - Information Technology Management Structure and Governance Framework
  - 38) M-08-27 - Guidance for Trusted Internet Connection (TIC) Compliance
  - 39) M-08-16 – Guidance for Trusted Internet Connection Statement of Capability Form (SOC)
  - 40) M-08-09 – New FISMA Privacy Reporting Requirements for FY 2008
  - 41) M-08-05 - Implementation of Trusted Internet Connections (TIC)
  - 42) M-08-01 - HSPD-12 Implementation Status
  - 43) M-07-18 - Ensuring New Acquisitions Include Common Security Configurations
  - 44) M-07-11 - Implementation of Commonly Accepted Security Configurations for Windows Operating Systems
  - 45) M-07-06 - Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials
  - 46) Recommendations for Identity Theft Related Data Breach Notification
  - 47) M-06-18 - Acquisition of Products and Services for Implementation of HSPD-12
  - 48) M-06-16 - Protection of Sensitive Agency Information
  - 49) M-06-06 - Sample Privacy Documents for Agency Implementation of Homeland Security Presidential Directive (HSPD) 12
  - 50) M-05-24 - Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors
  - 51) M05-16 - Regulation on Maintaining Telecommunication Services During a Crisis or Emergency in Federally-owned Buildings
  - 52) M-05-08 - Designation of Senior Agency Officials for Privacy
  - 53) M-05-05 - Electronic Signatures: How to Mitigate the Risk of Commercial Managed Services
  - 54) M-05-04 - Policies for Federal Agency Public Websites
  - 55) M-04-16 - Software Acquisition
  - 56) M-04-15 - Development of Homeland Security Presidential Directive (HSPD) - 7 Critical Infrastructure Protection Plans to Protect Federal Critical Infrastructures and Key Resources
  - 57) M-04-04 - E-Authentication Guidance for Federal Agencies
  - 58) M-03-22 - OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
  - 59) M-03-18 - Implementation Guidance for the E-Government Act of 2002
  - 60) M-02-09 - Reporting Instructions for the Government Information Security Reform Act and Updated Guidance on Security Plans of Action and Milestones
  - 61) M-02-01 - Guidance for Preparing and Submitting Security Plans of Action and Milestones
  - 62) M-01-05 - Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy
  - 63) M-00-13 - Privacy Policies and Data Collection on Federal Web Sites
  - 64) M-00-10 - OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act
  - 65) M-99-18 - Privacy Policies on Federal Web Sites

## 15. Department of Defense (DoD) Directives and Instructions

- 1) Department of Defense (DoD) Instruction 8500.01 - Cybersecurity
- 2) Department of Defense (DoD) Instruction 8510.01 - Risk Management Framework (RMF) for DoD Information Technology (IT)
- 3) Department of Defense (DoD) Directive 8000.01 - Management of the Department of Defense Information Enterprise (DoD IE)

- 
- 4) Department of Defense (DoD) Directive 8140.01 - Cyberspace Workforce Management

## 16. Committee on National Security Systems (CNSS) Publications

- 1) Committee on National Security Systems (CNSS) Publication (CNSSP) 22 - Cybersecurity Risk Management
- 2) Committee on National Security Systems Instruction (CNSSI) 1253 - Security Categorization and Control Selection for National Security Systems
- 3) Committee on National Security Systems Instruction (CNSSI) 1254 - Risk Management Framework Documentation, Data Element Standards, and Reciprocity Process for National Security Systems

## Domain 5 - NIST Risk Management Framework (formerly C&A)

The Risk Management Framework deals with system authorization and is in NIST Special Publication 800-37 Rev1 and supporting documents. These special publications and standards are downloadable at the following website: <http://csrc.nist.gov>.

1. 800-18 Rev1 - Guide for Developing Security Plans for Federal Information Systems
2. 800-30 Rev 1 - Guide for Conducting Risk Assessments
3. SP 800-34 Rev. 1 - Contingency Planning Guide for Federal Information Systems
4. 800-37 Rev1 - Guide for the Security Certification and Accreditation of Federal Information Systems
5. 800-37 Rev 2 - Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
6. 800-39 Managing Information Security Risk: Organization, Mission, and Information System View
7. 800-47 - Security Guide for Interconnecting Information Technology Systems
8. 800-53 Rev4 - Security and Privacy Controls for Federal Information Systems and Organizations
9. 800-53A Rev4 - Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans
10. 800-59 - Guideline for Identifying an Information System as a National Security System
11. 800-60 Rev1 - Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes)
12. 800-66 Rev1 - An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
13. 800-115 - Technical Guide to Information Security Testing and Assessment
14. 800-137 - Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
15. FIPS 200 - Minimum Security Requirements for Federal Information and Information Systems
16. FIPS 199 - Standards for Security Categorization of Federal Information and Information Systems

---

## Domain 6 - NIST Interagency Reports

NIST Interagency or Internal Reports (NISTIRs) describe research of a technical nature of interest to a specialized audience. These NISTIRs are downloadable at the following website: <http://csrc.nist.gov>.

1. NISTIR 8241 Organizational Views of NIST Cryptographic Standards and Testing and Validation Programs NISTIR 8240 Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process
2. NISTIR 8214 Threshold Schemes for Cryptographic Primitives: Challenges and Opportunities in Standardization and Validation of Threshold Cryptography
3. NISTIR 8202 Blockchain Technology Overview
4. NISTIR 8201 Internet of Things (IoT) Cybersecurity Colloquium: A NIST Workshop Proceedings
5. NISTIR 8200 Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT)
6. NISTIR 8194 Exploratory Lens Model of Decision-Making in a Potential Phishing Attack Scenario
7. NISTIR 8192 Enhancing Resilience of the Internet and Communications Ecosystem: a NIST Workshop Proceedings
8. NISTIR 8183 Cybersecurity Framework Manufacturing Profile
9. NISTIR 8179 Criticality Analysis Process Model: Prioritizing Systems and Components
10. NISTIR 8176 Security Assurance Requirements for Linux Application Container Deployments
11. NISTIR 8170 - The Cybersecurity Framework - Implementation Guidance for Federal Agencies
12. NISTIR 8062 - An Introduction to Privacy Engineering and Risk Management in Federal Systems
13. NISTIR 8060 - Guidelines for the Creation of Interoperable Software Identification (SWID) Tags
14. NISTIR 8053 - De-Identification of Personal Information
15. NISTIR 8011 Vol. 2 - Automation Support for Security Control Assessments: Hardware Asset Management
16. NISTIR 8011 Vol. 1 - Automation Support for Security Control Assessments: Overview
17. NISTIR 7946 - CVSS Implementation Guidance
18. NISTIR 7864 - The Common Misuse Scoring System (CMSS): Metrics for Software Feature Misuse Vulnerabilities
19. NISTIR 7800 - Applying the Continuous Monitoring Technical Reference Model to the Asset, Configuration, and Vulnerability Management Domains
20. NISTIR 7799 - Continuous Monitoring Reference Model Workflow, Subsystem, and Interface Specifications
21. NISTIR 7756 - CAESARS Framework Extension: An Enterprise Continuous Monitoring Technical Reference Architecture
22. NISTIR 7695 - Common Platform Enumeration: Naming Specification Version 2.3
23. NISTIR 7694 - Specification for Asset Reporting Format 1.1
24. NISTIR 7693 - Specification for Asset Identification 1.1
25. NISTIR 7692 - Specification for the Open Checklist Interactive Language (OCIL) Version 2.0
26. NISTIR 7622 - Notional Supply Chain Risk Management Practices for Federal Information Systems
27. NISTIR 7511 - Security Content Automation Protocol (SCAP) Version 1.2 Validation Program Test Requirements
28. NISTIR 7502 - The Common Configuration Scoring System (CCSS): Metrics for Software Security Configuration Vulnerabilities
29. NISTIR 7435 - The Common Vulnerability Scoring System (CVSS) and its Applicability to Federal Agency Systems
30. IR 7459 - Information Security Guide for Government Executives
31. IR 7358 - Program Review for Information Security Management Assistance (PRISMA)
32. IR 7298 - Glossary of Key Information Security Terms



---

## ***IT Security Topic Areas***

The purpose of this listing is to provide a basic understanding of key terms and concepts rather than offer an exhaustive list. Knowledge of these terms and concepts is the foundation for the effective performance of job functions associated with each of the management, operational, and technical topic areas.

Seventeen of the 18 IT Security topic areas come from the requirements defined in the Federal Information Processing Standard 200 (FIPS 200). One of the topic areas, Program Management, is new and comes from NIST SP 800-53 (Appendix G).

### **Topic Area 1 – Access Control**

This topic area refers to the knowledge and understanding that organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

<ul style="list-style-type: none"><li>• Access</li><li>• Access Authority</li><li>• Access Control</li><li>• Access Control List</li><li>• Account Management</li><li>• Access Enforcement</li><li>• Authorization</li><li>• Brute Force</li><li>• Concurrent Session Control</li><li>• Discretionary Access Control (DAC)</li><li>• Information Flow Enforcement</li></ul>	<ul style="list-style-type: none"><li>• Least Privilege</li><li>• Mandatory Access Control (MAC)</li><li>• Permitted Actions</li><li>• Previous Login Notification</li><li>• Role-Based Access Control (RBAC)</li><li>• Security Attributes</li><li>• Separation of Duties</li><li>• Session Lock</li><li>• Session Termination</li><li>• System Use Notification</li><li>• Unsuccessful Login Attempt</li></ul>
---	--

### **Topic Area 2 – Audit and Accountability**

This topic area refers to the knowledge and understanding that organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

<ul style="list-style-type: none"><li>• Accountability</li><li>• Auditable Event</li><li>• Audit</li><li>• Audit Analysis</li><li>• Audit Data</li></ul>	<ul style="list-style-type: none"><li>• Audit Review</li><li>• Audit Trail</li><li>• Audit Storage Capacity</li><li>• Audit Failure Response</li><li>• Contents of Audit Record</li></ul>
--	---

<ul style="list-style-type: none"> <li>• Audit Generation</li> <li>• Audit Policy</li> <li>• Audit Record Retention</li> <li>• Audit Reduction Tool</li> <li>• Audit Report</li> <li>• Audit Reduction</li> </ul>	<ul style="list-style-type: none"> <li>• Monitoring for Information Disclosure</li> <li>• Non-repudiation</li> <li>• Protection of Audit Information</li> <li>• Session Audit</li> <li>• Time Stamps</li> </ul>
---	---

**Topic Area 3 – Awareness and Training**

This topic area refers to the knowledge and understanding that organizations must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

<ul style="list-style-type: none"> <li>• Awareness (Information Security)</li> <li>• Behavioral Outcome</li> <li>• Certification</li> <li>• Computer-Based Training (CBT)</li> <li>• Curriculum</li> <li>• Education (Information Security)</li> <li>• End-User Security Training</li> <li>• Information Sharing</li> <li>• Instructional Systems Design (ISD)</li> <li>• Instructor-Led Training (ILT)</li> <li>• IT Security Awareness</li> <li>• IT Security Awareness and Training Program</li> </ul>	<ul style="list-style-type: none"> <li>• IT Security Education</li> <li>• IT Security Training Program</li> <li>• Learning Management System (LMS)</li> <li>• Learning Objectives</li> <li>• Needs Assessment (IT Security)</li> <li>• Role-Based Training</li> <li>• Testing</li> <li>• Training (Information Security)</li> <li>• Training Assessment</li> <li>• Training Effectiveness</li> <li>• Training Effectiveness Evaluation</li> <li>• Web-Based Training (WBT)</li> </ul>
---	---

**Topic Area 4 – Configuration Management**

This topic area refers to the knowledge and understanding that organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.

<ul style="list-style-type: none"> <li>• Access Restriction for Change</li> <li>• Baseline Configuration</li> <li>• Configuration Change</li> <li>• Configuration Management Plan</li> <li>• Configuration Management Policy</li> </ul>	<ul style="list-style-type: none"> <li>• Configuration Setting</li> <li>• United States Government Configuration Baseline (USGCB)”</li> <li>• Least Functionality</li> <li>• Security Checklists</li> <li>• Security Impact Analysis</li> </ul>
---	---

---

## Topic Area 5 – Contingency Planning

This topic area refers to the knowledge and understanding that organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

<ul style="list-style-type: none"><li>• Alternate Processing / Storage Site</li><li>• Backup Strategy</li><li>• Business Continuity Plan</li><li>• Business Impact Analysis</li><li>• Business Recovery Plan</li><li>• Call Tree</li><li>• Cold Site</li><li>• Contingency Plan</li><li>• Contingency Plan Policy</li><li>• Contingency Plan Training</li><li>• Contingency Plan Testing</li><li>• Continuity of Operations Plan</li><li>• Continuity of Support Plan</li><li>• Crisis Communication</li><li>• Cyber Incident Response</li><li>• Delegation of Authority</li><li>• Disaster Recovery Plan</li></ul>	<ul style="list-style-type: none"><li>• Disruption</li><li>• Essential Functions</li><li>• Hot Site</li><li>• Information Technology</li><li>• Interoperable Communications</li><li>• Mission Assurance</li><li>• Occupant Emergency Plan</li><li>• Order of Succession</li><li>• Preparedness/Readiness</li><li>• Reconstitution</li><li>• Recovery</li><li>• Risk Mitigation</li><li>• Standard Operating Procedures</li><li>• Telecommunications Services</li><li>• Threat Environment</li><li>• Vital Records and Databases</li><li>• Warm Site</li></ul>
---	---

## Topic Area 6 – Identification and Authentication

This topic area refers to the knowledge and understanding that organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

<ul style="list-style-type: none"><li>• Authenticate</li><li>• Authentication</li><li>• Authentication Mechanism</li><li>• Authentication Mode</li><li>• Authentication Protocol</li><li>• Authentication Token</li><li>• Authenticator Feedback</li><li>• Authenticator Management</li><li>• Authenticity</li><li>• Biometric</li><li>• Biometric System</li><li>• Biometric Information</li></ul>	<ul style="list-style-type: none"><li>• Device Identification</li><li>• Digital Certificate</li><li>• Certificate Policy</li><li>• Certificate Revocation List (CRL)</li><li>• Certification Authority</li><li>• Claimant</li><li>• Credential</li><li>• Cryptographic Module Authentication</li><li>• Electronic Authentication</li><li>• Identification</li><li>• Identifier Management</li><li>• Mutual Authentication</li></ul>
---	---

• Device Authentication	
-------------------------	--

## Topic Area 7 – Incident Response

This topic area refers to the knowledge and understanding that organizations must: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.

<ul style="list-style-type: none"> <li>• Attack Signature</li> <li>• Computer Forensics</li> <li>• Computer Security Incident</li> <li>• Computer Security Incident Response Team</li> <li>• Computer Security</li> <li>• Escalation Procedures</li> <li>• Honey Pot</li> <li>• Incident Handling</li> <li>• Incident Monitoring</li> <li>• Incident Records</li> <li>• Incident Reporting</li> <li>• Incident Response Assistance</li> <li>• Incident Response Plan</li> <li>• Incident Response Policy</li> </ul>	<ul style="list-style-type: none"> <li>• Incident Response Testing</li> <li>• Incident Response Training</li> <li>• Intrusion</li> <li>• Intrusion Prevention System</li> <li>• Intrusion Detection System</li> <li>• Measures</li> <li>• Personally Identifiable Information (PII)</li> <li>• Reconstitution of System</li> <li>• Security Alerts</li> <li>• Security Incident</li> <li>• System Compromise</li> <li>• Threat Motivation</li> <li>• Unauthorized Access</li> <li>• Vulnerability</li> </ul>
---	--

## Topic Area 8 – Maintenance

This topic area refers to the knowledge and understanding that organizations must: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

<ul style="list-style-type: none"> <li>• Antivirus Software</li> <li>• Backup</li> <li>• Baseline</li> <li>• Configuration Management</li> <li>• Controlled Maintenance</li> <li>• Insider Threat</li> <li>• Maintenance Tools</li> <li>• Maintenance Personnel</li> <li>• Non-Local Maintenance</li> <li>• Patch Management</li> <li>• Penetration Testing</li> </ul>	<ul style="list-style-type: none"> <li>• Security Data Analysis</li> <li>• Security Measures</li> <li>• Security Reporting</li> <li>• System Hardening</li> <li>• System Logs</li> <li>• System Maintenance Policy</li> <li>• System Monitoring</li> <li>• Threat Analysis</li> <li>• Threat Monitoring</li> <li>• Timely Maintenance</li> <li>• Vulnerability Analysis</li> </ul>
--	--

---

## Topic Area 9 – Media Protection

This topic area refers to the knowledge and understanding that organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.

<ul style="list-style-type: none"><li>• Degaussing</li><li>• Media Access</li><li>• Media Destruction &amp; Sanitization</li><li>• Media Marking</li></ul>	<ul style="list-style-type: none"><li>• Media Protection Policy</li><li>• Media Storage</li><li>• Media Transport</li><li>• Sanitization</li></ul>
--	--

## Topic Area 10 – Personnel Security

This topic area refers to the knowledge and understanding that organizations must: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

<ul style="list-style-type: none"><li>• Access Agreement</li><li>• Background Checks</li><li>• Background Investigation</li><li>• Confidentiality</li><li>• Digital Identity</li><li>• Human Resources</li><li>• Insider Threat</li><li>• Job Rotation</li><li>• Nondisclosure Agreement</li><li>• Position Categorization</li><li>• Position Sensitivity</li><li>• Personnel Sanctions</li></ul>	<ul style="list-style-type: none"><li>• Personnel Security Policy</li><li>• Personnel Screening</li><li>• Personnel Termination</li><li>• Personnel Transfer</li><li>• Security Breach</li><li>• Security Clearance</li><li>• Separation of Duties</li><li>• Social Engineering</li><li>• Special Background Investigation (SBI)</li><li>• Suitability Determination</li><li>• Third-Party Personnel Security</li></ul>
---	---

## Topic Area 11 – Physical and Environmental Protection

This topic area refers to the knowledge and understanding that organizations must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

<ul style="list-style-type: none"><li>• Access Cards</li><li>• Access Control</li></ul>	<ul style="list-style-type: none"><li>• Inventory</li></ul>
---	---

<ul style="list-style-type: none"> <li>• Access Control for Output Devices</li> <li>• Access Control for Transmission Medium</li> <li>• Access Records</li> <li>• Alarm</li> <li>• Alternate Work Site</li> <li>• Asset Disposal</li> <li>• Biometrics</li> <li>• Defense-in-Depth</li> <li>• Delivery and Removal</li> <li>• Emergency Lighting</li> <li>• Emergency Power</li> <li>• Environmental Threat</li> <li>• Fire Protection</li> <li>• Information Leakage</li> </ul>	<ul style="list-style-type: none"> <li>• Location of Information System Components</li> <li>• Manmade Threat</li> <li>• Monitoring Physical Access</li> <li>• Natural Threat</li> <li>• Perimeter Defense</li> <li>• Physical and Environmental Policy</li> <li>• Physical Access Authorization</li> <li>• Physical Access Control</li> <li>• Power Equipment and Power Cabling</li> <li>• Risk Management</li> <li>• Temperature and Humidity Control</li> <li>• Threat and Vulnerability Assessment</li> <li>• Video Surveillance</li> <li>• Visitor Control</li> <li>• Water Damage Protection</li> </ul>
--	--

## Topic Area 12 – Planning

This topic area refers to the knowledge and understanding that organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

<ul style="list-style-type: none"> <li>• Privacy Impact Assessment</li> <li>• Rules of Behavior</li> <li>• Security Planning Policy</li> </ul>	<ul style="list-style-type: none"> <li>• Security Planning Procedures</li> <li>• Security Related Activity Planning</li> <li>• System Security Plan</li> </ul>
--	--

## Topic Area 13 – Program Management

This topic area refers to the knowledge and understanding that organizations are required to implement security program management controls to provide a foundation for the organization’s information security program.

<ul style="list-style-type: none"> <li>• Critical Infrastructure Plan</li> <li>• Enterprise Architecture</li> <li>• Information Security Measures of Performance</li> <li>• Information Security Program Plan</li> <li>• Information Security Resources</li> </ul>	<ul style="list-style-type: none"> <li>• Information System Inventory</li> <li>• Mission/Business Process Definition</li> <li>• Security Authorization Process</li> <li>• Senior Information Security Officer</li> <li>• Plan of Action and Milestones Process</li> <li>• Risk Management Strategy</li> </ul>
--	---

---

## Topic Area 14 – Risk Assessment

This topic area refers to the knowledge and understanding that organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

<ul style="list-style-type: none"><li>• Acceptable Risk</li><li>• Assessment</li><li>• Asset Valuation</li><li>• Business Impact Analysis</li><li>• Controls</li><li>• Impact</li><li>• Inside Threat</li><li>• Likelihood Determination</li><li>• National Vulnerability Database</li><li>• Qualitative</li><li>• Quantitative</li><li>• Risk</li><li>• Risk Assessment</li><li>• Risk Assessment Policy</li><li>• Risk Avoidance</li><li>• Risk Level</li></ul>	<ul style="list-style-type: none"><li>• Risk Limitation</li><li>• Risk Management</li><li>• Risk Matrix</li><li>• Risk Mitigation</li><li>• Risk Research</li><li>• Risk Scale</li><li>• Risk Transference</li><li>• Security Categorization</li><li>• Security Controls</li><li>• Security Measures</li><li>• Threat</li><li>• Threat and Vulnerability</li><li>• Threat Modeling</li><li>• Types of Risk</li><li>• Vulnerability</li><li>• Vulnerability Scanning</li></ul>
---	---

## Topic Area 15 – Security Assessments and Authorization

*(Formerly Certification, Accreditation, and Security Assessments)*

This topic area refers to knowledge and understanding that organizations must: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

<ul style="list-style-type: none"> <li>• Assessment Method</li> <li>• Assessment Procedure</li> <li>• Authorization (to operate)</li> <li>• Authorization Boundary</li> <li>• Authorize Process</li> <li>• Authorizing Official</li> <li>• Designated Representative</li> <li>• Dynamic Subsystem</li> <li>• Common Control Provider</li> <li>• Common Control</li> <li>• Compensating Control</li> <li>• Complex Information System</li> <li>• Continuous Monitoring</li> <li>• Cost-Effective</li> <li>• Critical Control</li> <li>• External Subsystems</li> </ul>	<ul style="list-style-type: none"> <li>• Hybrid Security Control</li> <li>• Information Owner/Steward</li> <li>• Information System Boundary</li> <li>• Information System Owner</li> <li>• Information System Security Engineer</li> <li>• Information Type</li> <li>• Interconnection Agreement</li> <li>• Net-centric Architecture</li> <li>• Plan of Action and Milestones (POAM)</li> <li>• Reciprocity</li> <li>• Risk Executive</li> <li>• Security Control Assessor</li> <li>• Senior Information Security Officer</li> <li>• Tailored Security Control Baseline</li> <li>• Volatile Control</li> </ul>
---	---

## Topic Area 16 – System and Communication Protection

This topic area refers to the knowledge and understanding that organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

<ul style="list-style-type: none"> <li>• Application Partitioning</li> <li>• Boundary Protection</li> <li>• Collaborative Computing Devices</li> <li>• Communications Security</li> <li>• Configuration</li> <li>• Covert Channel Analysis</li> <li>• Cryptographic Key Establishment</li> <li>• Cryptographic Key Management</li> <li>• Defense-in-Depth</li> <li>• Denial of Service Protection</li> </ul>	<ul style="list-style-type: none"> <li>• Penetration Testing</li> <li>• Port</li> <li>• Protection of Information at Rest</li> <li>• Public Access Protections</li> <li>• Public Key Infrastructure Certificates</li> <li>• Resource Priority</li> <li>• Router</li> <li>• Secure Name Resolution</li> <li>• Security Function Isolation</li> <li>• Security Trust</li> </ul>
--	---



<ul style="list-style-type: none"> <li>• Emission Security</li> <li>• Encryption Technologies</li> <li>• Fail in Known State</li> <li>• Firewall</li> <li>• Heterogeneity</li> <li>• Honeypots</li> <li>• Hub</li> <li>• Information in Shared Resources</li> <li>• Information System Partitioning</li> <li>• Intrusion Detection System</li> <li>• Intrusion Prevention Systems</li> <li>• Load Balancers</li> <li>• Mobile Code</li> <li>• Network Architecture</li> <li>• Network Disconnect</li> <li>• Networking Models and Protocols</li> <li>• Network Segmentation</li> <li>• Non-Modifiable Executable Programs</li> </ul>	<ul style="list-style-type: none"> <li>• Session Authenticity</li> <li>• Switch</li> <li>• System and Communications Protection Policy</li> <li>• Telecommunications Technology</li> <li>• Thin Nodes</li> <li>• Transmission Confidentiality</li> <li>• Transmission of Security Attributes</li> <li>• Transmission Integrity</li> <li>• Transmission Preparation Integrity</li> <li>• Trusted Path</li> <li>• Use of Cryptography</li> <li>• Virtual Private Network (VPN)</li> <li>• VOIP</li> <li>• Virtualization Techniques</li> <li>• Vulnerability</li> <li>• Web Services Security</li> <li>• Wired and Wireless Networks</li> </ul>
--	---

## Topic Area 17 – System and Information Integrity

This topic area refers to the knowledge and understanding organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

<ul style="list-style-type: none"> <li>• Agent</li> <li>• Antivirus Software</li> <li>• Application</li> <li>• Application Content Filtering</li> <li>• Blended Attack</li> <li>• Boot Sector Virus</li> <li>• Buffer Overflow</li> <li>• Computer Virus</li> <li>• Error Handling</li> <li>• Flaw Remediation</li> <li>• Information Input Restrictions</li> </ul>	<ul style="list-style-type: none"> <li>• Information Input Validation</li> <li>• Information Output Handling and Retention</li> <li>• Information System Monitoring</li> <li>• Macro Virus</li> <li>• Malicious Code Protection</li> <li>• Predictable Failure Prevention</li> <li>• Security Alerts, Advisories, and Directives</li> <li>• Security Functionality Verification</li> <li>• Spam Protection</li> <li>• Software and Information Integrity</li> <li>• System and Information Integrity Policy</li> </ul>
---	--

## Topic Area 18 – System and Services Acquisition

This topic area refers to the knowledge and understanding that organizations must: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

---

<ul style="list-style-type: none"> <li>• Acquisitions</li> <li>• Allocation of Resources</li> <li>• Business Impact Analysis</li> <li>• Contract</li> <li>• Cost-Benefit Analysis</li> <li>• Critical Information System Components</li> <li>• Developer Configuration Management</li> <li>• Developer Security Testing</li> <li>• Disposal</li> <li>• External Information System Services</li> <li>• Information System Documentation</li> <li>• Life Cycle Support</li> <li>• Prequalification</li> <li>• Regulatory Compliance</li> <li>• Request for Information</li> <li>• Request for Proposal (RFP)</li> </ul>	<ul style="list-style-type: none"> <li>• Risk Analysis</li> <li>• Risk-Based Decision</li> <li>• Risk Mitigation</li> <li>• Security Engineering Principles</li> <li>• Security Requirements</li> <li>• Service Level Agreement (SLA)</li> <li>• System and Services Acquisition Policy</li> <li>• Software usage Restrictions</li> <li>• Solicitation</li> <li>• Supply Chain Protection</li> <li>• Statement of Objectives (SOO)</li> <li>• Statement of Work (SOW)</li> <li>• Total Cost of Ownership (TCO)</li> <li>• Trustworthiness</li> <li>• User Installed Software</li> </ul>
--	---

---

## 5. Appendix A – Rescinded Publications

### Domain 1 – NIST Special Publications

1. 800-13 - Telecommunications Security Guidelines for Telecommunications Management Network
2. 800-14- Generally Accepted Principles and Practices for Securing Information Technology Systems
3. 800-27 Rev A - Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
4. 800-33 - Underlying Technical Models for Information Technology Security
5. 800-36 - Guide to Selecting Information Technology Security Products
6. 800-65 - Integrating IT Security into the Capital Planning and Investment Control Process
7. 800-127 - Guide to Securing WiMAX Wireless Communications

### Domain 4 - Government Laws and Regulations

1. DHS Binding Operational Directives
  - a) BOD 15-01, Critical Vulnerability Mitigation Requirements for Federal Civilian Executive Branch Departments' and Agencies' Internet-Accessible Systems
  - b) BOD 16-01, Securing High Value Assets
2. Homeland Security Presidential Directives
  - a) HSPD-7 – Critical Infrastructure Identification, Prioritization, and Protection
3. OMB Memoranda
  - a) M-18-02, Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements
  - b) M-17-05, Fiscal Year 2016 - 2017 Guidance on Federal Information Security and Privacy Management Requirements
  - c) M-16-03, Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements
  - d) M-15-01, Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices
  - e) M-10-28, Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS)
  - f) M-10-15, FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
  - g) M-09-29 - FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
  - h) M-08-23 - Securing the Federal Government's Domain Name System Infrastructure
  - i) M-08-22 - Guidance on the Federal Desktop Core Configuration (FDCC)
  - j) M-08-21 – FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
  - k) M-07-19 – FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
  - l) M-07-16 - Safeguarding Against and Responding to the Breach of Personally Identifiable Information
  - m) Recommendations for Identity Theft Related Data Breach Notification

- 
- n) M-06-20 - FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
  - o) M-06-19 - Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments
  - p) M-06-15 - Safeguarding Personally Identifiable Information
  - q) M05-15 - FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
  - r) M-04-26 - Personal Use Policies and "File Sharing" Technology
  - s) M-04-25 - FY 2004 Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting
  - t) M-03-19 - FY 2003 Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting
  - u) M-01-24 - Reporting Instructions for the Government Information Security Reform Act
  - v) M-01-08 - Guidance on Implementing the Government Information Security Reform Act
  - w) M-00-07 - Incorporating and Funding Security in Information Systems Investments
  - x) M-00-01 - Day One Planning and Request for Updated Business Continuity and Contingency Plans
  - y) M-99-20 - Security of Federal Automated Information Resources
  - z) M-99-16 - Business Continuity and Contingency Planning for the Year 2000