Federal Body of Knowledge Guide

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

2010 Edition

This page is left intentionally blank

TABLE OF CONTENTS

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 will be updated annually and is meant to provide a high level description of the body of knowledge that is used as the basis of the exams.

This document is available free of charge at the FITSI website: http://www.fitsi.org. 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. FITSI produces Candidate Exam Guides (CEGs) for each certification role that customizes these documents and themes to a given role. Please refer to the FITSI website (http://www.fitsi.org) to download individual CEGs.

* The FBK incorporates themes, concepts and documents focused around unclassified federal information systems.

2. Relationship of the FITSI Exam Guides

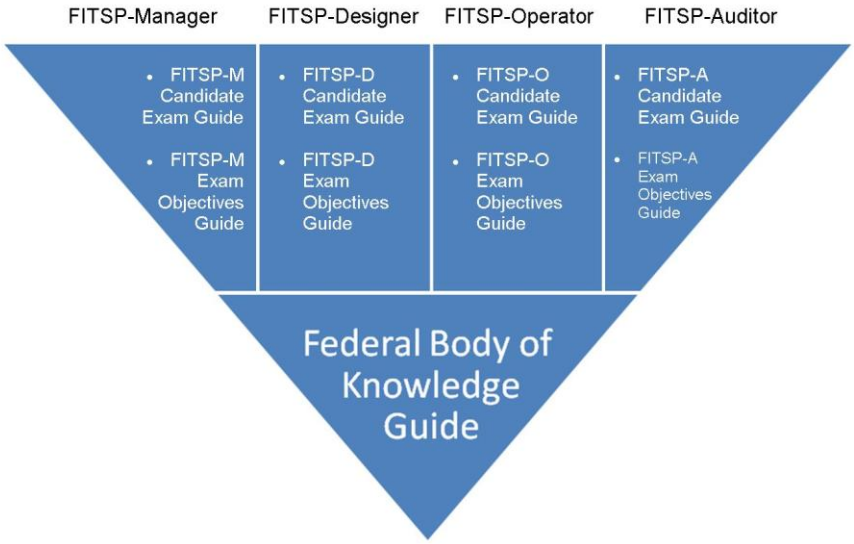
This guide is one of several documents published by FITSI to provide candidates with an understanding of the FITSP exam components. The three types of documents and their purposes are:

1. Candidate Exam Guide
   - Provides candidates with an overall understanding of the details of an exam for a particular FITSP certification role (Manager, Designer, Operator or Auditor).

2. Exam Objectives Guide
   - Provides the skills being measured and the exam objectives for a particular FITSP certification role (Manager, Designer, Operator or Auditor)

3. Federal Body of Knowledge Guide
   - Provides a detailed walkthrough of the set of domains, topics, publications and terminology that make up the FBK. This is an overarching document that provides the foundation for all the FITSP certification roles.

Below is a visual representation of how all these documents are interrelated:



3. FBK Overview

The FBK* is broken down into six domains and 21 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**

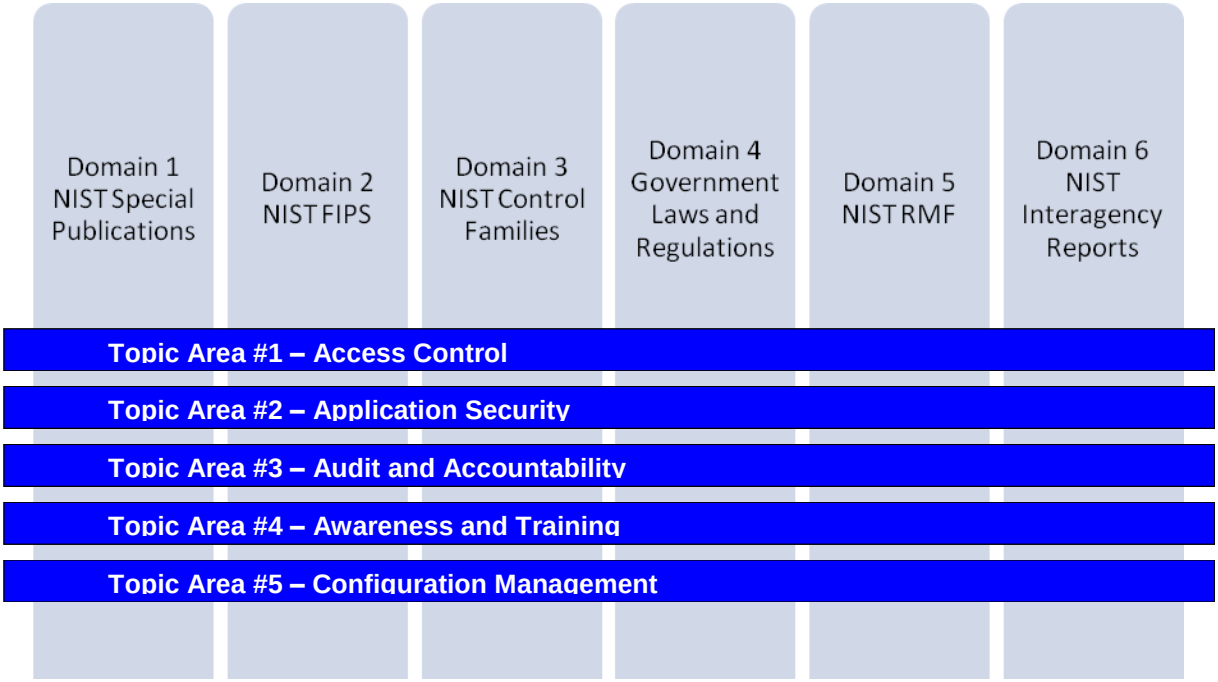
1. Access Control
2. Application Security
3. Audit and Accountability
4. Awareness and Training
5. Configuration Management
6. Contingency Planning
7. Data Security
8. Identification and Authentication
9. Incident Response
10. Maintenance
11. Media Protection
12. Personnel Security
13. Physical and Environmental Protection
14. Planning
15. Program Management
16. Regulatory and Standards Compliance
17. Risk Assessment
18. Security Assessment and Authorization
    a. (Formerly Certification, Accreditation, and Security Assessments)
19. System and Communications Protection
20. System and Information Integrity
21. System and Services Acquisition

* The FBK incorporates themes, concepts and documents focused around unclassified federal information systems.
** Seventeen of the 21 IT Security topic areas are derived directly from the minimum control requirements defined in Federal Information Processing Standard 200 (FIPS 200), one is defined in NIST SP 800-53 (Appendix G, Program Management) and three come from the Department of Homeland Security (DHS) Essential Body of Knowledge (EBK) IT security competencies.

4. How FITSP uses the FBK

Domains are the boundaries of knowledge that are applicable within 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 21 IT security topic areas (see illustration below).***

The interwoven nature of the domains and topic areas is represented below. Only five out of the 21 topic areas are listed for illustration purposes.



5. 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.

The reader is again reminded that this document serves simply as a reference on what constitutes the boundary of the FBK. FITSP candidates are not expected to review all documentation referenced herein but are recommended to download the Candidate Exam Guide (CEG) and/or the Exam Objectives Guide (EOG) for a specific certification role.

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 can be downloaded for free at the following website: http://csrc.nist.gov.

1. 800-12 -An Introduction to Computer Security: The NIST Handbook
2. 800-13 - Telecommunications Security Guidelines for Telecommunications Management Network
3. 800-14- Generally Accepted Principles and Practices for Securing Information Technology Systems
4. 800-16 - Information Technology Security Training Requirements: A Role- and Performance-Based Model
5. 800-18 Rev 1 - Guide for Developing Security Plans for Federal Information Systems
6. 800-21 2nd Ed - Guideline for Implementing Cryptography in the Federal Government
7. 800-23 - Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
8. 800-24 - PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does
9. 800-25 - Federal Agency Use of Public Key Technology for Digital Signatures and Authentication
10. 800-27 Rev A - Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
11. 800-28 Version 2 - Guidelines on Active Content and Mobile Code
12. 800- 30 - Risk Management Guide for Information Technology Systems
13. 800-32 - Introduction to Public Key Technology and the Federal PKI Infrastructure
14. 800-33 - Underlying Technical Models for Information Technology Security
15. 800-35 - Guide to Information Technology Security Services
16. 800-36 - Guide to Selecting Information Technology Security Products
17. 800-37 Rev 1 - Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
18. 800-40 Version 2 - Creating a Patch and Vulnerability Management Program
19. 800-41Rev 1 - Guidelines on Firewalls and Firewall Policy
20. 800-44 Version 2 - Guidelines on Securing Public Web Servers
21. 800-45 Version 2 - Guidelines on Electronic Mail Security
22. 800-46 Rev 1 - Guide to Enterprise Telework and Remote Access Security
23. 800-47 - Security Guide for Interconnecting Information Technology Systems
24. 800-48 Rev 1 - Guide to Securing Legacy IEEE 802.11 Wireless Networks
25. 800-49 - Federal S/MIME V3 Client Profile
26. 800-50 - Building an Information Technology Security Awareness and Training Program

27. 800-51 - Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme
28. 800-52 - Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations
29. 800-53 Rev3 - Recommended Security Controls for Federal Information Systems and Organizations
30. 800-53A - Guide for Assessing the Security Controls in Federal Information Systems
31. 800-55 Rev 1 - Performance Measurement Guide for Information Security
32. 800-56 A - Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
33. 800-57 - Recommendation for Key Management
34. 800-60 Rev 1 - Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) - Volume 1: Guide Volume 2: Appendices
35. 800-61 Rev 1 - Computer Security Incident Handling Guide
36. 800-63 Version 1.0.2 - Electronic Authentication Guideline
37. 800-64 Rev 2 – Security Considerations in the System Development Life Cycle
38. 800-65 - Integrating IT Security into the Capital Planning and Investment Control Process
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 1 - Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developer
41. 800-77 - Guide to IPSec VPNs
42. 800-78-2 - Cryptographic Algorithms and Key Sizes for Personal Identity Verification
43. 800-79-1 - Guidelines for the Accreditation of Personal Identity Verification (PIV) Card Issuers (PCI's)
44. 800-81 - Secure Domain Name System (DNS) Deployment Guide
45. 800-83 - Guide to Malware Incident Prevention and Handling
46. 800-84 - Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
47. 800-86 - Guide to Integrating Forensic Techniques into Incident Response
48. 800-87 Rev 1 - Codes for Identification of Federal and Federally-Assisted Organizations
49. 800-88 - Guidelines for Media Sanitization
50. 800-89 - Recommendation for Obtaining Assurances for Digital Signature Applications
51. 800-92 - Guide to Computer Security Log Management
52. 800-94 - Guide to Intrusion Detection and Prevention Systems (IDPS)
53. 800-95 - Guide to Secure Web Services
54. 800-96 - PIV Card to Reader Interoperability Guidelines
55. 800-97 - Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i
56. 800-98 - Guidelines for Securing Radio Frequency Identification (RFID) Systems
57. 800-100 - Information Security Handbook: A Guide for Managers
58. 800-107 - Recommendation for Applications Using Approved Hash Algorithms
59. 800-111 - Guide to Storage Encryption Technologies for End User Devices
60. 800-113 - Guide to SSL VPNs
61. 800-114 - User's Guide to Securing External Devices for Telework and Remote Access
62. 800-115 - Technical Guide to Information Security Testing and Assessment
63. 800-121 - Guide to Bluetooth Security
64. 800-123 - Guide to General Server Security
65. 800-124 - Guidelines on Cell Phone and PDA Security

Domain 2 - NIST Federal Information Processing Standards

Below is the list of all NIST Federal Information Processing Standards (FIPS) that are included in the FBK. These standards can be downloaded at the following website: http://csrc.nist.gov.

1. FIPS 201-1 - Personal Identity Verification (PIV) of Federal Employees and Contractors

2. FIPS 200 - Minimum Security Requirements for Federal Information and Information Systems
3. FIPS 199 - Standards for Security Categorization of Federal Information and Information Systems
4. FIPS 198-1 - The Keyed-Hash Message Authentication Code
5. FIPS 197 - Advanced Encryption Standard
6. FIPS 196 - Entity Authentication Using Public Key Cryptography
7. FIPS 191 - Guideline for the Analysis of Local Area Network Security
8. FIPS 190 - Guideline for the Use of Advanced Authentication Technology Alternatives
9. FIPS 188 - Standard Security Label for Information Transfer
10. FIPS 186-3 - Digital Signature Standard (DSS)
11. FIPS 185 - Escrowed Encryption Standard
12. FIPS 181 - Automated Password Generator
13. FIPS 180-3 - Secure Hash Standard (SHS)
14. FIPS 140-2 - Security Requirements for Cryptographic Modules
15. FIPS 113 - Computer Data Authentication (no electronic version available)

Domain 3 - NIST Control Families

NIST SP 800-53 Rev3 identifies 18 control families that must be incorporated into the design of federal systems. These control families are broken into three categories of controls (management, technical and operational).

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 at a number of Internet locations. OMB memos and bulletins can be obtained 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

2. OMB Memorandums

a) M-09-32 – Update on the Trusted Internet Connections Initiative
b) M-09-29 - FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
c) M-09-02 - Information Technology Management Structure and Governance Framework
d) M-08-27 - Guidance for Trusted Internet Connection (TIC) Compliance
e) M-08-23 - Securing the Federal Government's Domain Name System Infrastructure
f) M-08-22 - Guidance on the Federal Desktop Core Configuration (FDCC)
g) M-08-21 – FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
h) M-08-16 – Guidance for Trusted Internet Connection Statement of Capability Form (SOC)
i) M-08-09 – New FISMA Privacy Reporting Requirements for FY 2008
j) M-08-05 - Implementation of Trusted Internet Connections (TIC)
k) M-08-01 - HSPD-12 Implementation Status
l) M-07-19 – FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
m) M-07-18 - Ensuring New Acquisitions Include Common Security Configurations
n) M-07-16 - Safeguarding Against and Responding to the Breach of Personally Identifiable Information
o) M-07-11 - Implementation of Commonly Accepted Security Configurations for Windows Operating Systems
p) M-07-06 - Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials
q) Recommendations for Identity Theft Related Data Breach Notification
r) M-06-20 - FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
s) M-06-19 - Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments
t) M-06-18 - Acquisition of Products and Services for Implementation of HSPD-12
u) M-06-16 - Protection of Sensitive Agency Information
v) M-06-15 - Safeguarding Personally Identifiable Information
w) M-06-06 - Sample Privacy Documents for Agency Implementation of Homeland Security Presidential Directive (HSPD) 12
x) M-05-24 - Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors
y) M05-16 - Regulation on Maintaining Telecommunication Services During a Crisis or Emergency in Federally-owned Buildings
z) M05-15 - FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
a) M-05-08 - Designation of Senior Agency Officials for Privacy

b) M-05-05 - Electronic Signatures: How to Mitigate the Risk of Commercial Managed Services
c) M-05-04 - Policies for Federal Agency Public Websites
d) M-04-26 - Personal Use Policies and "File Sharing" Technology
e) M-04-25 – FY 2004 Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting
f) M-04-16 - Software Acquisition
g) M-04-15 - Development of Homeland Security Presidential Directive (HSPD) - 7 Critical Infrastructure Protection Plans to Protect Federal Critical Infrastructures and Key Resources
h) M-04-04 - E-Authentication Guidance for Federal Agencies
i) M-03-22 - OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
j) M-03-19 - FY 2003 Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting
k) M-03-18 - Implementation Guidance for the E-Government Act of 2002
l) M-02-09 - Reporting Instructions for the Government Information Security Reform Act and Updated Guidance on Security Plans of Action and Milestones
a) M-02-01 - Guidance for Preparing and Submitting Security Plans of Action and Milestones
b) M-01-24 - Reporting Instructions for the Government Information Security Reform Act
c) M-01-08 - Guidance on Implementing the Government Information Security Reform Act
d) M-01-05 - Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy
e) M-00-13 - Privacy Policies and Data Collection on Federal Web Sites
a) M-00-10 - OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act
b) M-00-07 - Incorporating and Funding Security in Information Systems Investments
c) M-00-01 - Day One Planning and Request for Updated Business Continuity and Contingency Plans
d) M-99-20 - Security of Federal Automated Information Resources
e) M-99-18 - Privacy Policies on Federal Web Sites
f) M-99-16 - Business Continuity and Contingency Planning for the Year 2000

3. OMB Circular

a) Office of Management and Budget Circular A-11, Preparation, Submission and Execution of the Budget, June 2008
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, Appendix III, Security of Federal Information Resources
e) Executive Office of the President, Office of Management and Budget, Office of Federal Procurement Policy, Emergency Acquisitions, May 2007

4. Homeland Security President Directives

a) HSPD-3 – Homeland Security Advisory System
b) HSPD-5 – Management of Domestic Incidents
c) HSPD-7 – Critical Infrastructure Identification, Prioritization, and Protection
d) HSPD-8 – National Preparedness
e) HSPD-12 – Policy for a Common Identification Standard for Federal Employees and Contractors
f) HSPD-20/NSPD-51 – National Continuity Policy
g) HSPD-24 – Biometrics for Identification and Screening to Enhance National Security

5. Executive Orders

    a) EO 12958 – Classified National Security Information
    b) 36 Code of Federal Regulation Part 1236, *Management of Vital Records*, revised as of July 1, 2000
    c) 41 Code of Federal Regulations 101.20.103-4, *Occupant Emergency Program*, revised as of July 1, 2000
    d) EO 12472 – Assignment of National Security and Emergency Preparedness Telecommunications Functions
    e) EO 12656 – Assignment of Emergency Preparedness Responsibilities
    f) EO 13231 – Critical Infrastructure Protection in the Information Age
    g) FCD 1 – Federal Executive Branch National Continuity Program and Requirements, Feb 2008
    h) FCD 2 – Federal Executive Branch Mission Essential function and Primary Mission Essential Function Identification and Submission Process, Feb 2008

6. 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)

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

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

1. 800-18 Rev1 - Guide for Developing Security Plans for Federal Information Systems
2. 800-34 - Contingency Planning Guide for Information Technology Systems
3. 800-47 - Security Guide for Interconnecting Information Technology Systems
4. 800-53 Rev3 - Recommended Security Controls for Federal Information Systems
5. 800-53A - Guide for Assessing the Security Controls in Federal Information Systems
6. 800-37 Rev1 - Guide for the Security Certification and Accreditation of Federal Information Systems
7. 800-59 - Guideline for Identifying an Information System as a National Security System
8. 800-60 Rev1- Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes)
9. 800-66 - An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
10. 800-115 - Technical Guide to Information Security Testing and Assessment
11. FIPS 200 - Minimum Security Requirements for Federal Information and Information Systems
12. 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 can be downloaded at the following website: http://csrc.nist.gov.

1. IR 7581 - System and Network Security Acronyms and Abbreviations
2. IR 7564 - Directions in Security Metrics Research
3. IR 7536 - 2008 Computer Security Division Annual Report
4. IR 7459 - Information Security Guide for Government Executives
5. IR 7358 - Program Review for Information Security Management Assistance (PRISMA)
6. IR 7316 - Assessment of Access Control Systems
7. IR 7298 - Glossary of Key Information Security Terms
8. IR 7206 - Smart Cards and Mobile Device Authentication: An Overview and Implementation

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 effective performance of job functions associated with each of the management, operational and technical topic areas.

Seventeen of the 21 IT Security topic areas are derived 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 Rev3 (Appendix G). Three of the topic areas (Application Security, Data Security and Regulatory and Standards Compliance) are derived from the DHS EBK.

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.

• Access	• Least Privilege
• Access Authority	• Mandatory Access Control (MAC)
• Access Control	• Permitted Actions
• Access Control List	• Previous Login Notification
• Account Management	• Role Based Access Control (RBAC)
• Access Enforcement	• Security Attributes
• Authorization	• Separation of Duties
• Brute Force	• Session Lock
• Concurrent Session Control	• Session Termination
• Discretionary Access Control (DAC)	• System Use Notification
• Information Flow Enforcement	• Unsuccessful Login Attempt

Topic Area 2 – Application Security

This topic area refers to the knowledge and understanding that organizations need to address security requirements in software development, handle the translation of security requirements into application design elements, and deal with the development of secure code and exploit mitigation.

• Application Controls	• Secure System Design
• Baseline Security	• Security Change Management
• Certification	• Security Requirements Analysis
• Configuration Management	• Security Specifications
• Patch Management	• Security Testing and Evaluation
• Process Maturity	• Security Vulnerability Analysis

• Risk Assessment • Risk Mitigation • Secure Coding • Secure Coding Principles • Secure Coding Tools	• Software Assurance • System Development Life Cycle (SDLC) • System Engineering • Technical Security Controls • Virtualization Technology

Topic Area 3 – 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.

• Accountability • Auditable Event • Audit • Audit Analysis • Audit Data • Audit Generation • Audit Policy • Audit Record Retention • Audit Reduction Tool • Audit Report • Audit Reduction	• Audit Review • Audit Trail • Audit Storage Capacity • Audit Failure Response • Contents of Audit Record • Monitoring for Information Disclosure • Non-repudiation • Protection of Audit Information • Session Audit • Time Stamps

Topic Area 4 – 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.

• Awareness (Information Security) • Behavioral Outcome • Certification • Computer Based Training (CBT) • Curriculum • Education (Information Security) • End User Security Training • Information Sharing • Instructional Systems Design (ISD)	• IT Security Education • IT Security Training Program • Learning Management System (LMS) • Learning Objectives • Needs Assessment (IT Security) • Role-Based Training • Testing • Training (Information Security) • Training Assessment

• Instructor Led Training (ILT) • IT Security Awareness • IT Security Awareness and Training Program	• Training Effectiveness • Training Effectiveness Evaluation • Web Based Training (WBT)

Topic Area 5 – 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.

• Access Restriction for Change • Baseline Configuration • Configuration Change • Configuration Management Plan • Configuration Management Policy	• Configuration Setting • Federal Desktop Core Configuration • Least Functionality • Security Checklists • Security Impact Analysis

Topic Area 6 – 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.

• Alternate Processing / Storage Site • Backup Strategy • Business Continuity Plan • Business Impact Analysis • Business Recovery Plan • Call Tree • Cold Site • Contingency Plan • Contingency Plan Policy • Contingency Plan Training • Contingency Plan Testing • Continuity of Operations Plan • Continuity of Support Plan • Crisis Communication • Cyber Incident Response • Delegation of Authority • Disaster Recovery Plan	• Disruption • Essential Functions • Hot Site • Information Technology • Interoperable Communications • Mission Assurance • Occupant Emergency Plan • Order of Succession • Preparedness/Readiness • Reconstitution • Recovery • Risk Mitigation • Standard Operating Procedures • Telecommunications Services • Threat Environment • Vital Records and Databases • Warm Site

Topic Area 7 – Data Security

This topic area refers to the knowledge and understanding that organizations must protect information and information systems at the appropriate level of confidentiality, integrity and availability.

• Access Control • Adequate Security • Aggregation • Antivirus Software • Assurance • Authentication • Authorization • Availability • Chain of Custody • Confidentiality • Data Classification • Decryption • Digital Signatures • Discretionary Access Control • Electronic Commerce • Encryption • Firewall Configuration • Identity Data and Access Management • Identity Management • Information Classification Scheme	• Integrity • Least Privilege • Mandatory Access Control • Need-to-Know • Non-repudiation • Personally Identifiable Information • Privacy • Privilege Levels • Public Key Infrastructure • Role-Based Access Control • Rule-Based Access Control • Secure Data Handling • Security Clearance • Sensitive Information • Sensitivity Determination • Sensitivity of Data • Steganography • System of Record • User Privileges • User Provisioning

Topic Area 8 – 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.

• Authenticate • Authentication • Authentication Mechanism • Authentication Mode • Authentication Protocol • Authentication Token • Authenticator Feedback • Authenticator Management • Authenticity • Biometric • Biometric System • Biometric Information • Device Authentication	• Device Identification • Digital Certificate • Certificate Policy • Certificate Revocation List (CRL) • Certification Authority • Claimant • Credential • Cryptographic Module Authentication • Electronic Authentication • Identification • Identifier Management • Mutual Authentication

Topic Area 9 – 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.

• Attack Signature	• Incident Response Testing
• Computer Forensics	• Incident Response Training
• Computer Security Incident	• Intrusion
• Computer Security Incident Response Team	• Intrusion Prevention System
• Computer Security	• Intrusion Detection System
• Escalation Procedures	• Measures
• Honey Pot	• Personally Identifiable Information (PII)
• Incident Handling	• Reconstitution of System
• Incident Monitoring	• Security Alerts
• Incident Records	• Security Incident
• Incident Reporting	• System Compromise
• Incident Response Assistance	• Threat Motivation
• Incident Response Plan	• Unauthorized Access
• Incident Response Policy	• Vulnerability

Topic Area 10 – 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.

• Antivirus Software	• Security Data Analysis
• Backup	• Security Measures
• Baseline	• Security Reporting
• Configuration Management	• System Hardening
• Controlled Maintenance	• System Logs
• Insider Threat	• System Maintenance Policy
• Maintenance Tools	• System Monitoring
• Maintenance Personnel	• Threat Analysis
• Non-Local Maintenance	• Threat Monitoring
• Patch Management	• Timely Maintenance
• Penetration Testing	• Vulnerability Analysis

Topic Area 11 – 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.

• Degaussing • Media Access • Media Destruction • Media Marking	• Media Protection Policy • Media Storage • Media Transport • Sanitization

Topic Area 12 – 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.

• Access Agreement • Background Checks • Background Investigation • Confidentiality • Digital Identity • Human Resources • Insider Threat • Job Rotation • Nondisclosure Agreement • Position Categorization • Position Sensitivity • Personnel Sanctions	• Personnel Security Policy • Personnel Screening • Personnel Termination • Personnel Transfer • Security Breach • Security Clearance • Separation of Duties • Social Engineering • Special Background Investigation (SBI) • Suitability Determination • Third-Party Personnel Security

Topic Area 13 – 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.

• Access Cards	• Inventory

• Access Control • Access Control for Output Devices • Access Control for Transmission Medium • Access Records • Alarm • Alternate Work Site • Asset Disposal • Biometrics • Defense-in-Depth • Delivery and Removal • Emergency Lighting • Emergency Power • Environmental Threat • Fire Protection • Information Leakage	• Location of Information System Components • Manmade Threat • Monitoring Physical Access • Natural Threat • Perimeter Defense • Physical and Environmental Policy • Physical Access Authorization • Physical Access Control • Power Equipment and Power Cabling • Risk Management • Temperature and Humidity Control • Threat and Vulnerability Assessment • Video Surveillance • Visitor Control • Water Damage Protection

Topic Area 14 – 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.

• Privacy Impact Assessment • Rules of Behavior • Security Planning Policy	• Security Planning Procedures • Security Related Activity Planning • System Security Plan

Topic Area 15 – 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.

• Critical Infrastructure Plan • Enterprise Architecture • Information Security Measures of Performance • Information Security Program Plan • Information Security Resources	• Information System Inventory • Mission/Business Process Definition • Security Authorization Process • Senior Information Security Officer • Plan of Action and Milestones Process • Risk Management Strategy

Topic Area 16 – Regulatory and Standards Compliance

This topic area refers to the application of principles, policies, and procedures that enable an organization to meet applicable information security laws, regulations, standards, and policies to satisfy statutory requirements, perform industry-wide best practices, and achieve information security program goals.

• Accountability • Assessment • Auditing • Certification • Compliance • Ethics • Evaluation • Governance • Laws	• Policy • Privacy Principles • Procedure • Regulations • Security Program • Standards • Validation • Verification

Topic Area 17 – 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.

• Acceptable Risk • Assessment • Asset Valuation • Business Impact Analysis • Controls • Impact • Inside Threat • Likelihood Determination • National Vulnerability Database • Qualitative • Quantitative • Risk • Risk Assessment • Risk Assessment Policy • Risk Avoidance • Risk Level	• Risk Limitation • Risk Management • Risk Matrix • Risk Mitigation • Risk Research • Risk Scale • Risk Transference • Security Categorization • Security Controls • Security Measures • Threat • Threat and Vulnerability • Threat Modeling • Types of Risk • Vulnerability • Vulnerability Scanning

Topic Area 18 – 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.

• Assessment Method • Assessment Procedure • Authorization (to operate) • Authorization Boundary • Authorize Process • Authorizing Official • Designated Representative • Dynamic Subsystem • Common Control Provider • Common Control • Compensating Control • Complex Information System • Continuous Monitoring • Cost Effective • Critical Control • External Subsytems	• Hybrid Security Control • Information Owner/Steward • Information System Boundary • Information System Owner • Information System Security Engineer • Information Type • Interconnection Agreement • Net-centric Architecture • Plan of Action and Milestones (POAM) • Reciprocity • Risk Executive • Security Control Assessor • Senior Information Security Officer • Tailored Security Control Baseline • Volatile Control

Topic Area 19 – 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.

• Application Partitioning • Boundary Protection • Collaborative Computing Devices • Communications Security • Configuration • Covert Channel Analysis • Cryptographic Key Establishment • Cryptographic Key Management • Defense-in-Depth	• Penetration Testing • Port • Protection of Information at Rest • Public Access Protections • Public Key Infrastructure Certificates • Resource Priority • Router • Secure Name Resolution • Security Function Isolation

• Denial of Service Protection • Emission Security • Encryption Technologies • Fail in Known State • Firewall • Heterogeneity • Honeypots • Hub • Information in Shared Resources • Information System Partitioning • Intrusion Detection System • Intrusion Prevention Systems • Load Balancers • Mobile Code • Network Architecture • Network Disconnect • Networking Models and Protocols • Network Segmentation • Non-Modifiable Executable Programs	• Security Trust • Session Authenticity • Switch • System and Communications Protection Policy • Telecommunications Technology • Thin Nodes • Transmission Confidentiality • Transmission of Security Attributes • Transmission Integrity • Transmission Preparation Integrity • Trusted Path • Use of Cryptography • Virtual Private Network (VPN) • VOIP • Virtualization Techniques • Vulnerability • Web Services Security • Wired and Wireless Networks

Topic Area 20 – 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.

• Agent • Antivirus Software • Application • Application Content Filtering • Blended Attack • Boot Sector Virus • Buffer Overflow • Computer Virus • Error Handling • Flaw Remediation • Information Input Restrictions	• Information Input Validation • Information Output Handling and Retention • Information System Monitoring • Macro Virus • Malicious Code Protection • Predictable Failure Prevention • Security Alerts, Advisories, and Directives • Security Functionality Verification • Spam Protection • Software and Information Integrity • System and Information Integrity Policy

Topic Area 21 – 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.

• Acquisitions • Allocation of Resources • Business Impact Analysis • Contract • Cost-Benefit Analysis • Critical Information System Components • Developer Configuration Management • Developer Security Testing • Disposal • External Information System Services • Information System Documentation • Life Cycle Support • Prequalification • Regulatory Compliance • Request for Information • Request for Proposal (RFP)	• Risk Analysis • Risk-Based Decision • Risk Mitigation • Security Engineering Principles • Security Requirements • Service Level Agreement (SLA) • System and Services Acquisition Policy • Software usage Restrictions • Solicitation • Supply Chain Protection • Statement of Objectives (SOO) • Statement of Work (SOW) • Total Cost of Ownership (TCO) • Trustworthiness • User Installed Software

6. FBK Updates

FITSI will provide an annual update to the FBK based upon newly released federal statutes, regulations, standards, and guidelines. This update occurs in January of a given year. As much of the content is derived from NIST documentation, draft documents are not incorporated into the FBK. Only current final versions are reviewed and included based on applicability.

FITSI members are asked to review the listing and provide commentary on possible changes that should be made to the FBK.

The following guidelines should be used in making recommendations:

1. The recommendation should be final (no draft documents)
2. The recommendation should be relevant (federal agencies and departments should be held accountable for its use)
3. The recommendation must be applicable to unclassified systems
4. The recommendation should focus on federal IT security.

Members are asked to submit recommended additions no later than December 15th, 2010 to the following email address: FBK@fitsi.org.