FITSP-Designer Candidate Exam Guide

An Overview of the
FITSP-D Certification

2010 Edition

This page is left intentionally blank

TABLE OF CONTENTS

1. Executive Overview

The FITSP-Designer Candidate Exam Guide (CEG) provides important logistical and procedural information for those wishing to take the FITSP-Designer exam. This guide is updated annually and provides a high level description of the body of knowledge that correlates to this exam.

Provided by the Federal IT Security Institute (FITSI), candidates can obtain this CEG free of charge at the Institute's website: http://www.fitsi.org. This document may be forwarded to professional colleagues but must be kept in its original form.

2. Relationship of the FITSI Exam Guides

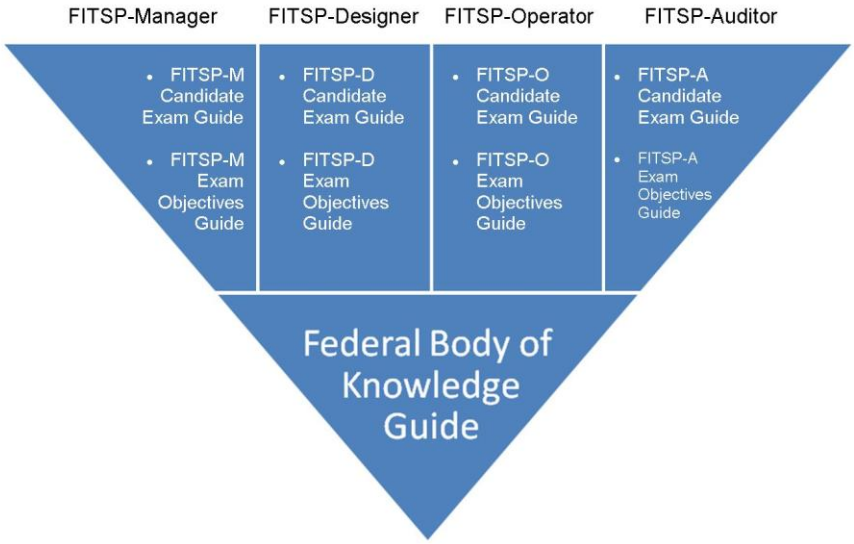
This guide is one of several documents published by FITSI to provide candidates with an understanding of the FITSP exam components. The three types of documents and their purposes are:

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. Intended Audience

The FITSP-Designer certification is intended for federal workforce personnel, both federal employees and contractors, whose role is primarily focused on the design and development of systems owned by, or operated on behalf of, the federal government of the United States. The following list highlights, but may not comprehensively capture, the commonly articulated roles characterized within federal statutory, regulatory, standards, and/or guidance documents that relate to the FITSP-Designer certification:

1) IT Security Engineer
2) Programmer
3) Security Engineer
4) System Designer
5) System Developer

Candidates are not required to be serving in one of these roles to pursue the FITSP-D certification. Anyone may pursue this credential provided they meet the necessary requirements as outlined later in this document.

4. Overview of the FITSP-Designer Certification

The FITSP-Designer certification is designed to demonstrate that federal workforce personnel, both federal employees and contractors, possess the knowledge of federal IT security requirements necessary to successfully design and develop the management, operational, and technical IT security controls for systems owned by, or operated on behalf of, the federal government. This role deals with high-level, cost-effective, risk-based IT security design functions that assure program value is achieved within the ever-changing risk and evolving threat environments.

Candidates are tested on a comprehensive Federal Body of Knowledge (FBK)*, which consists of a library of federal statutes, regulations, standards, and guidelines. 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

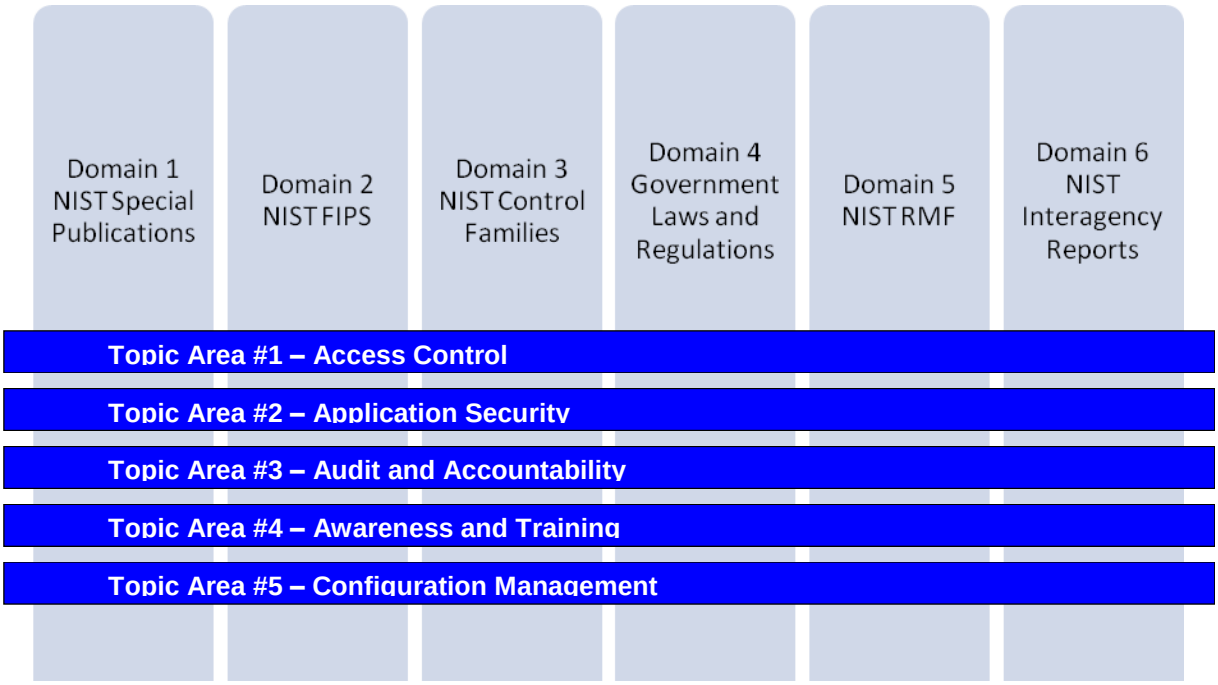
1. Access Control
2. Application Security
3. Audit and Accountability
4. Awareness and Training
5. Configuration Management
6. Contingency Planning
7. Data Security
8. Identification and Authentication
9. Incident Response
10. Maintenance
11. Media Protection
12. Personnel Security
13. Physical and Environmental 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.

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).***

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 (Program Management) and three come from the Department of Homeland Security (DHS) Essential Body of Knowledge (EBK) IT Security competencies.

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.



The following are the approximate areas of focus on which the FITSP-Designer candidate is tested:

Role	NIST Special Pubs	NIST FIPS	NIST Control Families	Laws and Regulations	NIST RMF	NIST IR
Designer	30%	10%	20%	10%	25%	5%

For a full listing of the FITSP-D skills measured, see the FITSP-Designer Exam Objectives Guide (EOG) found at the FITSI website. For a complete breakdown of the domains and topic areas see the Federal Body of Knowledge (FBK) Overview document found at the FITSI website.

5. Candidate Experience Requirements

Candidates must have five years of information systems security experience. This can be inside or outside the federal government. Candidates who pursue the FITSP certification can use both education and additional certifications to substitute for a number of years of experience.

Educational waivers – Candidates can waive one year of experience requirement with a four year accredited degree. This four year degree can be in any discipline. Candidates can waive two years of experience requirement with an accredited master's degree in IT security or information assurance.

Additional certifications – Candidates can waive one year of experience for each of the following certifications:

- CISM – Certified Information Security Manager
- CISSP – Certified Information Systems Security Professional
- CISA – Certified Information Systems Auditor
- GIAC – Global Information Assurance Certified
- CEH – Certified Ethical Hacker
- Security+
- SSCP – Systems Security Certified Practitioner
- SCNA – Security Certified Network Architect
- SCNP – Security Certified Network Professional
- SCNS – Security Certified Network Specialists
- CAP – Certification and Accreditation Professional

Candidates cannot waive more than three years of experience with any combination of education and or additional certifications. All candidates will need to provide proof of experience after passing the FITSP-D exam. This is accomplished through the FITSP-D application form that a candidate will fill out and submit after taking and passing the exam.

The application form requires a candidate to document their experience as well as have an employer or colleague attest to the background documented in the application. The application form is available at the FITSI website for download (http://www.fitsi.org).

6. Maintenance Requirements

All FITSP certifications are generally valid for three years but can be revoked by FITSI for violations of the Code of Ethics or other egregious acts that undermine the good character that must be demonstrated by a holder of a FITSP certification. FITSP certified members must earn Continuing Professional Education (CPE) units. Over the three-year period, a total of 60 CPEs must be earned, with a minimum of 20 CPEs to be earned each year. Once a member is certified, they will be provided a private account at the FITSI website to login and record annual CPE activities.

In additional to earning 60 CPEs over the three year period, FITSP certified members must pay a $45 annual certification maintenance fee to FITSI. If a FITSP candidate earns more than one FITSI certification they must earn 60 CPEs for each certification role but only must pay one $45 fee per year to FITSI (not per certification role).

7. Registration Requirements

Candidates can register for any of the FITSP certification exams at the FITSI website (http://www.fitsi.org). The following five steps must be taken:

1. Meet the minimum professional experience requirements
    a. See section 5 of this Candidate Exam Guide

2. Select one of the four certification roles
    a. Select FITSP-M, FITSP-D, FITSP-O, or FITSP-A
    b. See the FITSI website for more information

3. Sign up for an exam date and time
    a. See the FITSI website for available scheduling options

4. Agree to the FITSI Code of Ethics
    a. See section 8 of this Candidate Exam Guide

5. Pay for the exam
    a. See the FITSI website for more information

8. FITSI Code of Ethics

All candidates who pursue one of the four FITSP certification roles must agree to abide by the FITSI Code of Ethics. Below are the tenets that all members must agree to follow:

- Endeavor to protect the Nation's citizens, information systems, information, processes and facilities.
- Maintain a high level of personal integrity in any and all transactions with customers, stakeholders, colleagues and acquaintances.
- Maintain the confidentiality of all sensitive information (i.e.: Personally Identifiable Information) such that it does not create unnecessary risk for people and organizations.
- Refuse to engage in intentional activities that affect the availability of any and all IT systems and processes; both personally and professionally.
- Promote research and sharing of ideas and information that are worthy of such action. Give back to the community by adding value when possible.
- Refuse to foster FUD (Fear, Uncertainty and Doubt) in any and all interactions with both personal and professional relationships.
- Avoid conflicts of interest and recues oneself when appropriate.
- Mentor and teach whenever possible.

Violations of any of this Code of Ethics can be grounds for revocation of a member's certification(s) and/or membership in FITSI.

9. FITSP-Designer Documents from the Federal Body of Knowledge (FBK)*

The FITSP-Designer certification is broken down into six domains and 21 IT security topic areas. The purpose of this section is to provide the reader with an idea of the FBK that a candidate must be familiar with in preparation for the exam.

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.

IT Security Topic Areas Special Publications:

1. **Access Control**
   800-12 – An Introduction to Computer Security: The NIST Handbook
2. **Application Security**
   800-12 – An Introduction to Computer Security: The NIST Handbook
3. **Audit and Accountability**
   800-92, Guide to Computer Security Log Management
4. **Awareness and Training**
   800-16 - Information Technology Security Training Requirements: A Role- and Performance-Based Model
   800-50 - Building an Information Technology Security Awareness and Training Program
5. **Configuration Management**
   800-40, Version 2, Creating a Patch and Vulnerability Management Program
6. **Contingency Planning**
   800-34, Contingency Planning Guide for Information Technology Systems
7. **Data Security**
   800-12 – An Introduction to Computer Security: The NIST Handbook
   800-60 Rev1 - Guide for Mapping Types of Information and Information Systems to Security Categories
8. **Identification and Authentication**
   800-63 - Electronic Authentication Guideline
9. **Incident Response**
   800-61 - Computer Security Incident Handling Guide
10. **Maintenance**
    800-12 – An Introduction to Computer Security: The NIST Handbook
11. **Media Protection**
    800-88 - Guidelines for Media Sanitization
12. **Personnel Security**
    800-12 – An Introduction to Computer Security: The NIST Handbook
13. **Physical and Environmental Protection**
    800-12 - An Introduction to Computer Security: The NIST Handbook

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

14. **Planning**
    800-18 - Guide for Developing Security Plans for Federal Information Systems
15. **Program Management**
    800-53 Rev3 - Recommended Security Controls for Federal Information Systems and Organizations - (Appendix G)
16. **Regulatory and Standards Compliance**
    800-12 – An Introduction to Computer Security: The NIST Handbook
17. **Risk Assessment**
    800-30 - Risk Management Guide for Information Technology Systems
18. **Security Assessments and Authorization**
    800-37 Rev1- Guide for Applying the Risk Management Framework to Federal Information Systems
19. **System and Communication Protection**
    800-13 - Telecommunications Security Guidelines for Telecommunications Management Network
20. **System and Information Integrity**
    800-12 - An Introduction to Computer Security: The NIST Handbook
21. **System and Services Acquisition**
    800-36 - Guide to Selecting Information Security Products

Role-based Special Publications (per design role identified in NIST SP 800-16 Rev1)

1. 800-53 Rev3- Recommended Security Controls for Federal Information Systems and Organizations
2. 800-64 Rev 2 – Security Considerations in the System Development Life Cycle
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. 800-53A - Guide for Assessing the Security Controls in Federal Information Systems
6. 800-100 - Information Security Handbook: A Guide for Managers

Additional Special Publications (added by FITSI)

1. 800-32 - Introduction to Public Key Technology and the Federal PKI Infrastructure
2. 800-41Rev 1 - Guidelines on Firewalls and Firewall Policy
3. 800-45 Version 2 - Guidelines on Electronic Mail Security
4. 800-47 - Security Guide for Interconnecting Information Technology Systems
5. 800-52 - Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations
6. 800-57 - Recommendation for Key Management
7. 800-70 Rev 1 - Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developer
8. 800-77 - Guide to IPSec VPNs
9. 800-95 - Guide to Secure Web Services
10. 800-113 - Guide to SSL VPNs

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 directives 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-8-23 - 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-01-05 - Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy
c) 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-130, Appendix III, Security of Federal Information Resources
b) 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

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