Guide to NIST Information Security Documents

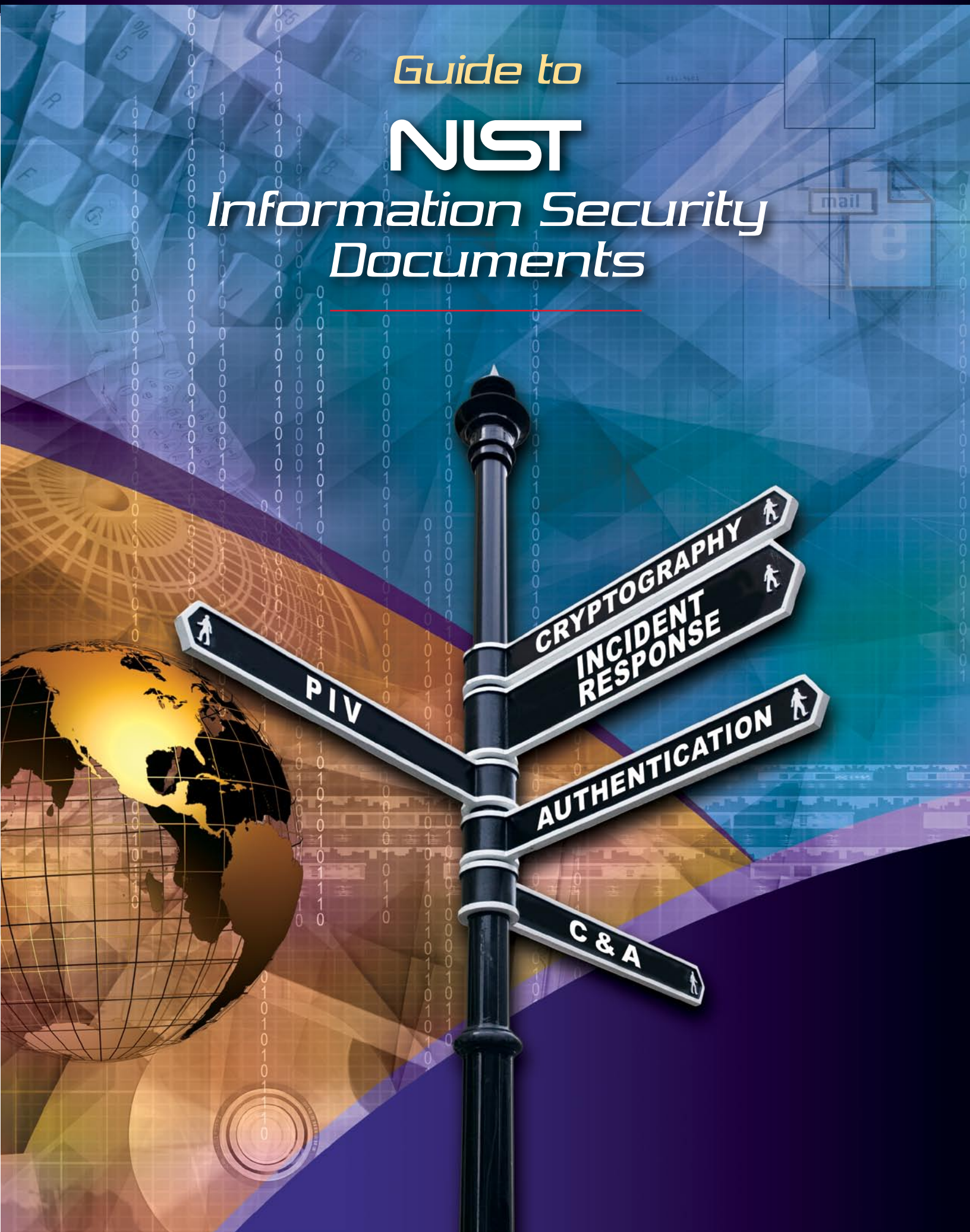

Table of Contents

Introduction **1**
Topic Clusters **2**
Annual Reports 2
Audit & Accountability 2
Authentication 3
Awareness & Training 4
Biometrics 4
Certification & Accreditation (C&A) 5
Communications & Wireless 6
Contingency Planning 6
Cryptography 7
Digital Signatures 8
Forensics 8
General IT Security 8
Incident Response 9
Maintenance 9
Personal Identity Verification (PIV) 10
PKI 11
Planning 11
Research 13
Risk Assessment 13
Services & Acquisitions 14
Smart Cards 15
Viruses & Malware 15
Historical Archives 16
Families **18**
Access Control 18
Awareness & Training 19
Audit & Accountability 19
Certification, Accreditation & Security Assessments 19
Configuration Management 20
Contingency Planning 21
Identification & Authentication 21
Incident Response 22
Maintenance 22
Media Protection 23
Physical & Environmental Protection 23
Planning 23
Personnel Security 24
Risk Assessment 25
System & Services Acquisition 26
System & Communication Protection 26
System & Information Integrity 28
Legal Requirements **29**
Federal Information Security Management Act of 2002 (FISMA) 29
OMB Circular A-130: Management of Federal Information Resources, Appendix III: Security of Federal Automated Information Resources 30
E-Government Act of 2002 31
Homeland Security Presidential Directive-12 (HSPD-12), Common Identification Standard for Federal Employees and Contractors 31
OMB Circular A–11: Preparation, Submission, and Execution of the Budget 31
Other Requirements with Supporting Documents 32
Health Insurance Portability and Accountability Act (HIPAA) 32
Homeland Security Presidential Directive-7 (HSPD-7), Critical Infrastructure Identification, Prioritization, and Protection 32

Introduction

For many years, the Computer Security Division has made great contributions to help secure our nation's information and information systems. Our work has paralleled the evolution of information technology (IT), initially focused principally on mainframe computers, to now encompass today's wide gamut of (IT) devices.

Currently, there are over 250 NIST information security documents. This number includes Federal Information Processing Standards (FIPS), the Special Publication (SP) 800 series, Information Technology Laboratory (ITL) Bulletins, and NIST Interagency Reports (NISTIR). These documents are typically listed by publication type and number or by month and year in the case of the ITL Bulletins. This can make finding a document difficult if the number or date is not known.

In order to make NIST information security documents more accessible, especially to those just entering the security field or with limited needs for the documents, we are presenting this Guide. In addition to being listed by type and number, this will present the documents using three approaches to ease searching:

- by Topic Cluster
- by Family
- by Legal Requirement

Several people looking for documents regarding Federal employee identification badges might approach their search in drastically different ways. One person might look for the legal basis behind the badges, HSPD-12 (Homeland Security Presidential Directive 12). HSPD-12 is listed in the legal requirement list. Another might look for "PIV" (personal identification verification), and they could find it under the topic clusters. Another might look for "Identification and Authentication," and they would find it under the family list. Yet another person might look for "smart card" or "biometrics," both of which are under the topic clusters.

It needs to be understood, however, that documents are not generally mapped to every topic mentioned in the document. For instance, SP 800-66, *An Introductory Resource Guide for implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule* deals with topics such as contingency plans and incident response. However, SP 800-66 is not considered an essential document when looking for documents about contingency plans or incident response.

The Guide will be updated on a bi-annual basis to include new documents, topic clusters, and legal requirements, as well as to update any shifts in document mapping that is appropriate.

NIST INFORMATION SECURITY DOCUMENTS

The **Federal Information Processing Standards** (FIPS) Publication Series is the official series of publications relating to standards and guidelines adopted and promulgated under the provisions of the Federal Information Security Management Act (FISMA) of 2002.

The **Special Publication 800-series** reports on ITL's research, guidelines, and outreach efforts in information system security and its collaborative activities with industry, government, and academic organizations.

ITL Bulletins are published by the Information Technology Laboratory. Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. Bulletins are issued on an as-needed basis.

The NIST **Interagency Report** series may report results of projects of transitory or limited interest. They may also include interim or final reports on work performed by NIST for outside sponsors (both government and non-government).

Topic Clusters

ANNUAL REPORTS

The Annual Reports are the method that the NIST Computer Security Division uses to publicly report on the past year's accomplishments and plans for the next year.

NISTIR 7285	Computer Security Division - 2005 Annual Report
NISTIR 7219	Computer Security Division - 2004 Annual Report
NISTIR 7111	Computer Security Division - 2003 Annual Report

AUDIT & ACCOUNTABILITY

A collection of documents that relates to review and examination of records and activities in order to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to provide the supporting requirement for actions of an entity to be traced uniquely to that entity.

FIPS 200	Security Controls for Federal Information Systems
FIPS 199	Standards for Security Categorization of Federal Information and Information Systems
FIPS 191	Guideline for The Analysis of Local Area Network Security
FIPS 140-2	Security Requirements for Cryptographic Modules
SP 800-92	Guide to Computer Security Log Management
SP 800-55	Security Metrics Guide for Information Technology Systems
SP 800-53A	Guide for Assessing the Security Controls in Federal Information Systems
SP 800-53	Security Controls for Federal Information Systems
SP 800-50	Building an Information Technology Security Awareness and Training Program
SP 800-42	Guideline on Network Security Testing
SP 800-41	Guidelines on Firewalls and Firewall Policy
SP 800-37	Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems
SP 800-30	Risk Management Guide for Information Technology Systems
SP 800-26	Security Self-Assessment Guide for Information Technology Systems
SP 800-18	Guide for Developing Security Plans for Information Technology Systems
SP 800-16	Information Technology Security Training Requirements: A Role- and Performance-Based Model
NISTIR 7316	Assessment of Access Control Systems
NISTIR 7284	Personal Identity Verification Card Management Report
NISTIR 6981	Policy Expression and Enforcement for Handheld Devices

(continued on next page)

AUDIT & ACCOUNTABILITY CONTINUED

March 2006	Minimum Security Requirements For Federal Information And Information Systems: Federal Information Processing Standard (FIPS) 200 Approved By The Secretary Of Commerce
January 2006	Testing And Validation Of Personal Identity Verification (PIV) Components And Subsystems For Conformance To Federal Information Processing Standard 201
August 2005	Implementation Of FIPS 201, Personal Identity Verification (PIV) Of Federal Employees And Contractors
May 2005	Recommended Security Controls For Federal Information Systems: Guidance For Selecting Cost-Effective Controls Using A Risk-Based Process
November 2004	Understanding the New NIST Standards and Guidelines Required by FISMA: How Three Mandated Documents are Changing the Dynamic of Information Security for the Federal Government
March 2004	Federal Information Processing Standard (FIPS) 199, Standards For Security Categorization Of Federal Information And Information Systems
August 2003	IT Security Metrics
June 2003	ASSET: Security Assessment Tool For Federal Agencies
January 2002	Guidelines on Firewalls and Firewall Policy
September 2001	Security Self-Assessment Guide for Information Technology Systems
February 2000	Guideline for Implementing Cryptography in the Federal Government

AUTHENTICATION

FIPS 198	The Keyed-Hash Message Authentication Code (HMAC)
FIPS 196	Entity Authentication Using Public Key Cryptography
FIPS 190	Guideline for the Use of Advanced Authentication Technology Alternatives
FIPS 186-3	Digital Signature Standard (DSS)
FIPS 181	Automated Password Generator
FIPS 180-2	Secure Hash Standard (SHS)
SP 800-89	Recommendation for Obtaining Assurances for Digital Signature Applications
SP 800-63	Recommendation for Electronic Authentication
SP 800-57	Recommendation on Key Management
SP 800-38C	Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality
SP 800-38B	Recommendation for Block Cipher Modes of Operation: The RMAC Authentication Mode
SP 800-38A	Recommendation for Block Cipher Modes of Operation - Methods and Techniques
SP 800-32	Introduction to Public Key Technology and the Federal PKI Infrastructure
SP 800-25	Federal Agency Use of Public Key Technology for Digital Signatures and Authentication
SP 800-21 Rev 1	Guideline for Implementing Cryptography in the Federal Government
SP 800-17	Modes of Operation Validation System (MOVS): Requirements and Procedures
NISTIR 7290	Fingerprint Identification and Mobile Handheld Devices: An Overview and Implementation
NISTIR 7206	Smart Cards and Mobile Device Authentication: An Overview and Implementation
NISTIR 7200	Proximity Beacons and Mobile Handheld Devices: Overview and Implementation
NISTIR 7046	Framework for Multi-Mode Authentication: Overview and Implementation Guide

(continued on next page)

AUTHENTICATION CONTINUED

NISTIR 7030	Picture Password: A Visual Login Technique for Mobile Devices
September 2005	Biometric Technologies: Helping To Protect Information And Automated Transactions In Information Technology Systems
July 2005	Protecting Sensitive Information That Is Transmitted Across Networks: NIST Guidance For Selecting And Using Transport Layer Security Implementations
August 2004	Electronic Authentication: Guidance For Selecting Secure Techniques
March 2003	Security For Wireless Networks And Devices
May 2001	Biometrics - Technologies for Highly Secure Personal Authentication
March 2001	An Introduction to IPsec (Internet Protocol Security)

AWARENESS & TRAINING

SP 800-66	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
SP 800-50	Building an Information Technology Security Awareness and Training Program
SP 800-46	Security for Telecommuting and Broadband Communications
SP 800-16	Information Technology Security Training Requirements: A Role- and Performance-Based Model
NISTIR 7284	Personal Identity Verification Card Management Report
October 2003	Information Technology Security Awareness, Training, Education, and Certification
November 2002	Security For Telecommuting And Broadband Communications

BIOMETRICS

A collection of documents that details security issues and potential controls using a measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of a person.

FIPS 201-1	Personal Identity Verification for Federal Employees and Contractors
SP 800-76	Biometric Data Specification for Personal Identity Verification
NISTIR 7290	Fingerprint Identification and Mobile Handheld Devices: An Overview and Implementation
NISTIR 7284	Personal Identity Verification Card Management Report
NISTIR 7206	Smart Cards and Mobile Device Authentication: An Overview and Implementation
NISTIR 7056	Card Technology Development and Gap Analysis Interagency Report
NISTIR 6887	Government Smart Card Interoperability Specification (GSC-IS), v2.1
NISTIR 6529-A	Common Biometric Exchange File Format (CBEFF)
September 2005	Biometric Technologies: Helping To Protect Information And Automated Transactions In Information Technology Systems
August 2005	Implementation Of FIPS 201, Personal Identity Verification (PIV) Of Federal Employees And Contractors
March 2005	Personal Identity Verification (PIV) Of Federal Employees And Contractors: Federal Information Processing Standard (FIPS) 201
July 2002	Overview: The Government Smart Card Interoperability Specification
May 2001	Biometrics - Technologies for Highly Secure Personal Authentication

CERTIFICATION & ACCREDITATION (C&A)

Certification and Accreditation (C&A) is a collection of documents that can be used to conduct the C&A of an information system in accordance with OMB A130-III.

FIPS 200	Security Controls for Federal Information Systems
FIPS 199	Standards for Security Categorization of Federal Information and Information Systems
FIPS 191	Guideline for The Analysis of Local Area Network Security
SP 800-88	Media Sanitization Guide
SP 800-84	Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
SP 800-60	Guide for Mapping Types of Information and Information Systems to Security Categories
SP 800-59	Guideline for Identifying an Information System as a National Security System
SP 800-55	Security Metrics Guide for Information Technology Systems
SP 800-53A	Guide for Assessing the Security Controls in Federal Information Systems
SP 800-53	Security Controls for Federal Information Systems
SP 800-47	Security Guide for Interconnecting Information Technology Systems
SP 800-42	Guideline on Network Security Testing
SP 800-37	Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems
SP 800-34	Contingency Planning Guide for Information Technology Systems
SP 800-30	Risk Management Guide for Information Technology Systems
SP 800-26	Security Self-Assessment Guide for Information Technology Systems
SP 800-23	Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
SP 800-18	Guide for Developing Security Plans for Information Technology Systems
March 2006	Minimum Security Requirements For Federal Information And Information Systems: Federal Information Processing Standard (FIPS) 200 Approved By The Secretary Of Commerce
May 2005	Recommended Security Controls For Federal Information Systems: Guidance For Selecting Cost-Effective Controls Using A Risk-Based Process
November 2004	Understanding the New NIST Standards and Guidelines Required by FISMA: How Three Mandated Documents are Changing the Dynamic of Information Security for the Federal Government
July 2004	Guide For Mapping Types Of Information And Information Systems To Security Categories
May 2004	Guide For The Security Certification And Accreditation Of Federal Information Systems
March 2004	Federal Information Processing Standard (FIPS) 199, Standards For Security Categorization Of Federal Information And Information Systems
August 2003	IT Security Metrics
June 2003	ASSET: Security Assessment Tool For Federal Agencies
February 2003	Secure Interconnections for Information Technology Systems
September 2001	Security Self-Assessment Guide for Information Technology Systems

COMMUNICATIONS & WIRELESS

A collection of documents that details security issues associated with the transmission of information over multiple media to include security considerations with the use of wireless.

FIPS 140-2	Security Requirements for Cryptographic Modules
SP 800-82	Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security
SP 800-81	Secure Domain Name System (DNS) Deployment Guide
SP 800-77	Guide to IPsec VPNs
SP 800-58	Security Considerations for Voice Over IP Systems
SP 800-52	Guidelines for the Selection and Use of Transport Layer Security
SP 800-48	Wireless Network Security: 802.11, Bluetooth, and Handheld Devices
SP 800-46	Security for Telecommuting and Broadband Communications
SP 800-45	Guidelines on Electronic Mail Security
SP 800-41	Guidelines on Firewalls and Firewall Policy
SP 800-24	PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does
NISTIR 7206	Smart Cards and Mobile Device Authentication: An Overview and Implementation
NISTIR 7046	Framework for Multi-Mode Authentication: Overview and Implementation Guide
October 2004	Securing Voice Over Internet Protocol (IP) Networks
March 2003	Security For Wireless Networks And Devices
January 2003	Security Of Electronic Mail
November 2002	Security For Telecommuting And Broadband Communications
January 2002	Guidelines on Firewalls and Firewall Policy
March 2001	An Introduction to IPsec (Internet Protocol Security)
August 2000	Security for Private Branch Exchange Systems

CONTINGENCY PLANNING

A collection of documents that details management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.

SP 800-84	Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
SP 800-46	Security for Telecommuting and Broadband Communications
SP 800-34	Contingency Planning Guide for Information Technology Systems
January 2004	Computer Security Incidents: Assessing, Managing, And Controlling The Risks
June 2002	Contingency Planning Guide For Information Technology Systems
April 2002	Techniques for System and Data Recovery

CRYPTOGRAPHY

A collection of documents that discusses the multiple uses and security issues of encryption, decryption, key management, and the science and technologies used to assure the confidentiality of information by hiding semantic content, preventing unauthorized use, or preventing undetected modification.

FIPS 198	The Keyed-Hash Message Authentication Code (HMAC)
FIPS 197	Advanced Encryption Standard
FIPS 196	Entity Authentication Using Public Key Cryptography
FIPS 190	Guideline for the Use of Advanced Authentication Technology Alternatives
FIPS 186-3	Digital Signature Standard (DSS)
FIPS 185	Escrowed Encryption Standard
FIPS 181	Automated Password Generator
FIPS 180-2	Secure Hash Standard (SHS)
FIPS 140-2	Security Requirements for Cryptographic Modules
SP 800-90	Recommendation for Random Number Generation Using Deterministic Random Bit Generators
SP 800-67	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
SP 800-57	Recommendation on Key Management
SP 800-56A	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
SP 800-52	Guidelines on the Selection and Use of Transport Layer Security
SP 800-49	Federal S/MIME V3 Client Profile
SP 800-38C	Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality
SP 800-38B	Recommendation for Block Cipher Modes of Operation: The RMAC Authentication Mode
SP 800-38A	Recommendation for Block Cipher Modes of Operation - Methods and Techniques
SP 800-32	Introduction to Public Key Technology and the Federal PKI Infrastructure
SP 800-25	Federal Agency Use of Public Key Technology for Digital Signatures and Authentication
SP 800-22	A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications
SP 800-21 Rev 1	Guideline for Implementing Cryptography in the Federal Government
SP 800-17	Modes of Operation Validation System (MOVS): Requirements and Procedures
SP 800-15	Minimum Interoperability Specification for PKI Components (MISPC), Version 1
NISTIR 7206	Smart Cards and Mobile Device Authentication: An Overview and Implementation
NISTIR 7046	Framework for Multi-Mode Authentication: Overview and Implementation Guide
September 2002	Cryptographic Standards and Guidelines: A Status Report
December 2000	A Statistical Test Suite For Random And Pseudorandom Number Generators For Cryptographic Applications
February 2000	Guideline for Implementing Cryptography in the Federal Government

DIGITAL SIGNATURES

A collection of documents that discusses the multiple uses and security issues of digital signatures.

FIPS 198	The Keyed-Hash Message Authentication Code (HMAC)
FIPS 186-3	Digital Signature Standard (DSS)
FIPS 180-2	Secure Hash Standard (SHS)
FIPS 140-2	Security Requirements for Cryptographic Modules
SP 800-57	Recommendation on Key Management
SP 800-52	Guidelines on the Selection and Use of Transport Layer Security
SP 800-49	Federal S/MIME V3 Client Profile
SP 800-32	Introduction to Public Key Technology and the Federal PKI Infrastructure
SP 800-25	Federal Agency Use of Public Key Technology for Digital Signatures and Authentication
SP 800-21 Rev 1	Guideline for Implementing Cryptography in the Federal Government
SP 800-15	Minimum Interoperability Specification for PKI Components (MISPC), Version 1
February 2000	Guideline for Implementing Cryptography in the Federal Government

FORENSICS

A collection of documents that discusses the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

SP 800-86	Guide to Integrating Forensic Techniques into Incident Response
SP 800-72	Guidelines on PDA Forensics
SP 800-31	Intrusion Detection Systems (IDSs)
NISTIR 7250	Cell Phone Forensic Tools: An Overview and Analysis
NISTIR 7100	PDA Forensic Tools: An Overview and Analysis
September 2006	Forensic Techniques: Helping Organizations Improve Their Responses To Information Security Incidents
November 2001	Computer Forensics Guidance

GENERAL IT SECURITY

A collection of documents that spans multiple topic areas and covers a very broad range of security subjects. These documents are not typically listed in Topic Clusters because they are generally applicable to almost all of them.

FIPS 200	Security Controls for Federal Information Systems
SP 800-100	Information Security Handbook for Managers
SP 800-64	Security Considerations in the Information System Development Life Cycle
SP 800-47	Security Guide for Interconnecting Information Technology Systems
SP 800-33	Underlying Technical Models for Information Technology Security
SP 800-27	Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
SP 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems
SP 800-12	An Introduction to Computer Security: The NIST Handbook
NISTIR 7298	Glossary of Key Information Security Terms

INCIDENT RESPONSE

A collection of documents to assist in the creation of a pre-determined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attack against an organization's IT system(s).

SP 800-86	Guide to Integrating Forensic Techniques into Incident Response
SP 800-84	Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
SP 800-83	Guide to Malware Incident Prevention and Handling
SP 800-61	Computer Security Incident Handling Guide
SP 800-51	Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme
SP 800-40	Procedures for Handling Security Patches
SP 800-31	Intrusion Detection Systems (IDSs)
NISTIR 7250	Cell Phone Forensic Tools: An Overview and Analysis
NISTIR 7100	PDA Forensic Tools: An Overview and Analysis
NISTIR 6981	Policy Expression and Enforcement for Handheld Devices
NISTIR 6416	Applying Mobile Agents to Intrusion Detection and Response
September 2006	Forensic Techniques: Helping Organizations Improve Their Responses To Information Security Incidents
February 2006	Creating A Program To Manage Security Patches And Vulnerabilities: NIST Recommendations For Improving System Security
December 2005	Preventing And Handling Malware Incidents: How To Protect Information Technology Systems From Malicious Code And Software
October 2005	National Vulnerability Database: Helping Information Technology System Users And Developers Find Current Information About Cyber Security Vulnerabilities
January 2004	Computer Security Incidents: Assessing, Managing, And Controlling The Risks
October 2002	Security Patches And The CVE Vulnerability Naming Scheme: Tools To Address Computer System Vulnerabilities
April 2002	Techniques for System and Data Recovery
November 2001	Computer Forensics Guidance

MAINTENANCE

A collection of documents discussing security concerns with systems in the maintenance phase of the System Development Life Cycle.

SP 800-88	Media Sanitization Guide
SP 800-84	Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
SP 800-83	Guide to Malware Incident Prevention and Handling
SP 800-70	Security Configuration Checklists Program for IT Products
SP 800-69	Guidance for Securing Microsoft Windows XP Home Edition: a NIST Security Configuration Checklist
SP 800-68	Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist
SP 800-55	Security Metrics Guide for Information Technology Systems
SP 800-53	Security Controls for Federal Information Systems
SP 800-51	Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme
SP 800-44	Guidelines on Securing Public Web Servers
SP 800-43	Systems Administration Guidance for Securing Microsoft Windows 2000 Professional System
SP 800-41	Guidelines on Firewalls and Firewall Policy

(continued on next page)

MAINTENANCE CONTINUED

SP 800-40	Procedures for Handling Security Patches
SP 800-31	Intrusion Detection Systems (IDSs)
SP 800-24	PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does
NISTIR 7284	Personal Identity Verification Card Management Report
NISTIR 7275	Specification for the Extensible Configuration Checklist Description Format (XCCDF)
NISTIR 6985	COTS Security Protection Profile - Operating Systems (CSPP-OS) (Worked Example Applying Guidance of NISTIR-6462, CSPP)
NISTIR 6462	CSPP - Guidance for COTS Security Protection Profiles
FIPS 191	Guideline for The Analysis of Local Area Network Security
FIPS 188	Standard Security Labels for Information Transfer
December 2005	Preventing And Handling Malware Incidents: How To Protect Information Technology Systems From Malicious Code And Software
February 2006	Creating A Program To Manage Security Patches And Vulnerabilities: NIST Recommendations For Improving System Security
November 2005	Securing Microsoft Windows XP Systems: NIST Recommendations For Using A Security Configuration Checklist
October 2005	National Vulnerability Database: Helping Information Technology System Users And Developers Find Current Information About Cyber Security Vulnerabilities
October 2004	Securing Voice Over Internet Protocol (IP) Networks
January 2004	Computer Security Incidents: Assessing, Managing, And Controlling The Risks
November 2003	Network Security Testing
December 2002	Security of Public Web Servers
October 2002	Security Patches And The CVE Vulnerability Naming Scheme: Tools To Address Computer System Vulnerabilities
January 2002	Guidelines on Firewalls and Firewall Policy

PERSONAL IDENTITY VERIFICATION (PIV)

Personal Identity Verification (PIV) is a suite of standards and guides that are developed in response to HSPD-12 for improving the identification and authentication of Federal employees and contractors for access to Federal facilities and information systems.

FIPS 201-1	Personal Identity Verification for Federal Employees and Contractors
SP 800-85B	PIV Data Model Test Guidelines
SP 800-85A	PIV Card Application and Middleware Interface Test Guidelines (SP800-73 compliance)
SP 800-79	Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations
SP 800-78	Cryptographic Algorithms and Key Sizes for Personal Identity Verification
SP 800-76	Biometric Data Specification for Personal Identity Verification
SP 800-73 Rev 1	Integrated Circuit Card for Personal Identification Verification
NISTIR 7337	Personal Identity Verification Demonstration Summary
NISTIR 7284	Personal Identity Verification Card Management Report
January 2006	Testing And Validation Of Personal Identity Verification (PIV) Components And Subsystems For Conformance To Federal Information Processing Standard 201
August 2005	Implementation Of FIPS 201, Personal Identity Verification (PIV) Of Federal Employees And Contractors
March 2005	Personal Identity Verification (PIV) Of Federal Employees And Contractors: Federal Information Processing Standard (FIPS) 201

PKI

A collection of documents to assist with the understanding of Public Key cryptography.

FIPS 196	Entity Authentication Using Public Key Cryptography
SP 800-89	Recommendation for Obtaining Assurances for Digital Signature Applications
SP 800-57	Recommendation on Key Management
SP 800-32	Introduction to Public Key Technology and the Federal PKI Infrastructure
SP 800-25	Federal Agency Use of Public Key Technology for Digital Signatures and Authentication
SP 800-15	Minimum Interoperability Specification for PKI Components (MISPC), Version 1

PLANNING

A collection of documents dealing with security plans and for identifying, documenting, and preparing security for systems.

FIPS 200	Security Controls for Federal Information Systems
FIPS 199	Standards for Security Categorization of Federal Information and Information Systems
FIPS 191	Guideline for The Analysis of Local Area Network Security
FIPS 188	Standard Security Labels for Information Transfer
FIPS 140-2	Security Requirements for Cryptographic Modules
SP 800-81	Secure Domain Name System (DNS) Deployment Guide
SP 800-57	Recommendation on Key Management
SP 800-55	Security Metrics Guide for Information Technology Systems
SP 800-53	Security Controls for Federal Information Systems
SP 800-47	Security Guide for Interconnecting Information Technology Systems
SP 800-44	Guidelines on Securing Public Web Servers
SP 800-43	Systems Administration Guidance for Securing Microsoft Windows 2000 Professional System
SP 800-41	Guidelines on Firewalls and Firewall Policy
SP 800-40, Ver 2	Creating a Patch and Vulnerability Management Program
SP 800-37	Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems
SP 800-36	Guide to Selecting Information Technology Security Products
SP 800-35	Guide to Information Technology Security Services
SP 800-33	Underlying Technical Models for Information Technology Security
SP 800-32	Introduction to Public Key Technology and the Federal PKI Infrastructure
SP 800-31	Intrusion Detection Systems (IDSs)
SP 800-30	Risk Management Guide for Information Technology Systems
SP 800-27	Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
SP 800-25	Federal Agency Use of Public Key Technology for Digital Signatures and Authentication
SP 800-21 Rev 1	Guideline for Implementing Cryptography in the Federal Government
SP 800-19	Mobile Agent Security

(continued on next page)

PLANNING CONTINUED

SP 800-18	Guide for Developing Security Plans for Information Technology Systems
NISTIR 7316	Assessment of Access Control Systems
NISTIR 7284	Personal Identity Verification Card Management Report
NISTIR 6985	COTS Security Protection Profile - Operating Systems (CSPP-OS) (Worked Example Applying Guidance of NISTIR-6462, CSPP)
NISTIR 6981	Policy Expression and Enforcement for Handheld Devices
NISTIR 6887	Government Smart Card Interoperability Specification (GSC-IS), v2.1
NISTIR 6462	CSPP - Guidance for COTS Security Protection Profiles
December 2005	Preventing And Handling Malware Incidents: How To Protect Information Technology Systems From Malicious Code And Software
March 2006	Minimum Security Requirements For Federal Information And Information Systems: Federal Information Processing Standard (FIPS) 200 Approved By The Secretary Of Commerce
February 2006	Creating A Program To Manage Security Patches And Vulnerabilities: NIST Recommendations For Improving System Security
January 2006	Testing And Validation Of Personal Identity Verification (PIV) Components And Subsystems For Conformance To Federal Information Processing Standard 201
November 2005	Securing Microsoft Windows XP Systems: NIST Recommendations For Using A Security Configuration Checklist
August 2005	Implementation Of FIPS 201, Personal Identity Verification (PIV) Of Federal Employees And Contractors
July 2005	Protecting Sensitive Information That Is Transmitted Across Networks: NIST Guidance For Selecting And Using Transport Layer Security Implementations
June 2005	NIST's Security Configuration Checklists Program For IT Products
May 2005	Recommended Security Controls For Federal Information Systems: Guidance For Selecting Cost-Effective Controls Using A Risk-Based Process
January 2005	Integrating It Security Into The Capital Planning And Investment Control Process
November 2004	Understanding the New NIST Standards and Guidelines Required by FISMA: How Three Mandated Documents are Changing the Dynamic of Information Security for the Federal Government
July 2004	Guide For Mapping Types Of Information And Information Systems To Security Categories
May 2004	Guide For The Security Certification And Accreditation Of Federal Information Systems
March 2004	Federal Information Processing Standard (FIPS) 199, Standards For Security Categorization Of Federal Information And Information Systems
February 2003	Secure Interconnections for Information Technology Systems
December 2002	Security of Public Web Servers
July 2002	Overview: The Government Smart Card Interoperability Specification
February 2002	Risk Management Guidance For Information Technology Systems
January 2002	Guidelines on Firewalls and Firewall Policy
February 2000	Guideline for Implementing Cryptography in the Federal Government
April 1999	Guide for Developing Security Plans for Information Technology Systems

RESEARCH

A collection of documents that reports on the techniques and results of security research subjects, topics, forums or workshops.

NISTIR 7224	4th Annual PKI R&D Workshop: Multiple Paths to Trust – Proceedings
NISTIR 7200	Proximity Beacons and Mobile Handheld Devices: Overview and Implementation
NISTIR 7056	Card Technology Development and Gap Analysis Interagency Report
NISTIR 7007	An Overview of Issues in Testing Intrusion Detection Systems
NISTIR 6068	Report on the TMACH Experiment
NISTIR 5810	The TMACH Experiment Phase 1 - Preliminary Developmental Evaluation
NISTIR 5788	Public Key Infrastructure Invitational Workshop September 28, 1995, MITRE Corporation, McLean, Virginia
July 2003	Testing Intrusion Detection Systems

RISK ASSESSMENT

A collection of documents that assists in identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact.

FIPS 199	Standards for Security Categorization of Federal Information and Information Systems
FIPS 191	Guideline for The Analysis of Local Area Network Security
SP 800-84	Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
SP 800-60	Guide for Mapping Types of Information and Information Systems to Security Categories
SP 800-51	Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme
SP 800-48	Wireless Network Security: 802.11, Bluetooth, and Handheld Devices
SP 800-47	Security Guide for Interconnecting Information Technology Systems
SP 800-42	Guideline on Network Security Testing
SP 800-40, Ver 2	Creating a Patch and Vulnerability Management Program
SP 800-37	Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems
SP 800-30	Risk Management Guide for Information Technology Systems
SP 800-28	Guidelines on Active Content and Mobile Code
SP 800-26	Security Self-Assessment Guide for Information Technology Systems
SP 800-23	Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
SP 800-21 Rev 1	Guideline for Implementing Cryptography in the Federal Government
SP 800-19	Mobile Agent Security
NISTIR 7316	Assessment of Access Control Systems
NISTIR 6981	Policy Expression and Enforcement for Handheld Devices
February 2006	Creating A Program To Manage Security Patches And Vulnerabilities: NIST Recommendations For Improving System Security
October 2005	National Vulnerability Database: Helping Information Technology System Users And Developers Find Current Information About Cyber Security Vulnerabilities
May 2005	Recommended Security Controls For Federal Information Systems: Guidance For Selecting Cost-Effective Controls Using A Risk-Based Process

(continued on next page)

RISK ASSESSMENT CONTINUED

July 2004	Guide For Mapping Types Of Information And Information Systems To Security Categories
May 2004	Guide For The Security Certification And Accreditation Of Federal Information Systems
March 2004	Federal Information Processing Standard (FIPS) 199, Standards For Security Categorization Of Federal Information And Information Systems
January 2004	Computer Security Incidents: Assessing, Managing, And Controlling The Risks
November 2003	Network Security Testing
February 2003	Secure Interconnections for Information Technology Systems
October 2002	Security Patches And The CVE Vulnerability Naming Scheme: Tools To Address Computer System Vulnerabilities
February 2002	Risk Management Guidance For Information Technology Systems
September 2001	Security Self-Assessment Guide for Information Technology Systems

SERVICES & ACQUISITIONS

A collection of documents to assist with understanding security issues concerning purchasing and obtaining items. Also covers considerations for acquiring services, including assistance with a system at any point in its life cycle, from external sources.

FIPS 201-1	Personal Identity Verification for Federal Employees and Contractors
FIPS 140-2	Security Requirements for Cryptographic Modules
SP 800-97	Guide to IEEE 802.11i: Robust Security Networks
SP 800-85	PIV Middleware and PIV Card Application Conformance Test Guidelines
SP 800-79	Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations
SP 800-78	Cryptographic Algorithms and Key Sizes for Personal Identity Verification
SP 800-76	Biometric Data Specification for Personal Identity Verification
SP 800-73 Rev 1	Integrated Circuit Card for Personal Identification Verification
SP 800-70	Security Configuration Checklists Program for IT Products
SP 800-66	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
SP 800-65	Integrating Security into the Capital Planning and Investment Control Process
SP 800-58	Security Considerations for Voice Over IP Systems
SP 800-48	Wireless Network Security: 802.11, Bluetooth, and Handheld Devices
SP 800-36	Guide to Selecting Information Technology Security Products
SP 800-35	Guide to Information Technology Security Services
SP 800-25	Federal Agency Use of Public Key Technology for Digital Signatures and Authentication
SP 800-21 Rev 1	Guideline for Implementing Cryptography in the Federal Government
SP 800-15	Minimum Interoperability Specification for PKI Components (MISPC), Version 1
NISTIR 7284	Personal Identity Verification Card Management Report
NISTIR 7250	Cell Phone Forensic Tools: An Overview and Analysis
NISTIR 7100	PDA Forensic Tools: An Overview and Analysis
NISTIR 6887	Government Smart Card Interoperability Specification (GSC-IS), v2.1

(continued on next page)

SERVICES & ACQUISITIONS CONTINUED

January 2006	Testing And Validation Of Personal Identity Verification (PIV) Components And Subsystems For Conformance To Federal Information Processing Standard 201
August 2005	Implementation Of FIPS 201, Personal Identity Verification (PIV) Of Federal Employees And Contractors
June 2005	NIST's Security Configuration Checklists Program For IT Products
March 2005	Personal Identity Verification (PIV) Of Federal Employees And Contractors: Federal Information Processing Standard (FIPS) 201
January 2005	Integrating It Security Into The Capital Planning And Investment Control Process
October 2004	Securing Voice Over Internet Protocol (IP) Networks
June 2004	Information Technology Security Services: How To Select, Implement, And Manage
April 2004	Selecting Information Technology Security Products
July 2002	Overview: The Government Smart Card Interoperability Specification
February 2000	Guideline for Implementing Cryptography in the Federal Government

SMART CARDS

A collection of documents that provides information on cards with built-in microprocessors and memory that can be used for identification purposes.

FIPS 201-1	Personal Identity Verification for Federal Employees and Contractors
SP 800-85A	PIV Card Application and Middleware Interface Test Guidelines (SP800-73 compliance)
SP 800-73 Rev 1	Integrated Circuit Card for Personal Identification Verification
NISTIR 7284	Personal Identity Verification Card Management Report
NISTIR 7206	Smart Cards and Mobile Device Authentication: An Overview and Implementation
NISTIR 7056	Card Technology Development and Gap Analysis Interagency Report
NISTIR 6887	Government Smart Card Interoperability Specification (GSC-IS), v2.1
January 2006	Testing And Validation Of Personal Identity Verification (PIV) Components And Subsystems For Conformance To Federal Information Processing Standard 201
August 2005	Implementation Of FIPS 201, Personal Identity Verification (PIV) Of Federal Employees And Contractors
March 2005	Personal Identity Verification (PIV) Of Federal Employees And Contractors: Federal Information Processing Standard (FIPS) 201
July 2002	Overview: The Government Smart Card Interoperability Specification

VIRUSES & MALWARE

A collection of documents that deals with viruses, malware, and how to handle them.

SP 800-83	Guide to Malware Incident Prevention and Handling
SP 800-61	Computer Security Incident Handling Guide
SP 800-28	Guidelines on Active Content and Mobile Code
SP 800-19	Mobile Agent Security

HISTORICAL ARCHIVES

NIST documents that are now obsolete or nearly obsolete, due to changes in technologies and/or environments, or documents that have had newer versions published, thereby making these obsolete. These are listed here mostly for academic and historical purposes.

SP 800-29	A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2
SP 800-13	Telecommunications Security Guidelines for Telecommunications Management Network
SP 800-11	The Impact of the FCC's Open Network Architecture on NS/EP Telecommunications Security
SP 800-10	Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls
SP 800-09	Good Security Practices for Electronic Commerce, Including Electronic Data Interchange
SP 800-08	Security Issues in the Database Language SQL
SP 800-07	Security in Open Systems
SP 800-06	Automated Tools for Testing Computer System Vulnerability
SP 800-05	A Guide to the Selection of Anti-Virus Tools and Techniques
SP 800-04	Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators
SP 800-03	Establishing a Computer Security Incident Response Capability (CSIRC)
SP 800-02	Public-Key Cryptography
NISTIR 6483	Randomness Testing of the Advanced Encryption Standard Finalist Candidates
NISTIR 6390	Randomness Testing of the Advanced Encryption Standard Candidate Algorithms
NISTIR 5590	Proceedings Report of the International Invitation Workshop on Developmental Assurance
NISTIR 5570	An Assessment of the DOD Goal Security Architecture (DGSA) for Non-Military Use
NISTIR 5540	Multi-Agency Certification and Accreditation (C&A) Process: A Worked Example
NISTIR 5495	Computer Security Training & Awareness Course Compendium
NISTIR 5472	A Head Start on Assurance Proceedings of an Invitational Workshop on Information Technology (IT) Assurance and Trustworthiness
NISTIR 5308	General Procedures for Registering Computer Security Objects
NISTIR 5283	Security of SQL-Based Implementations of Product Data Exchange Using Step
NISTIR 5234	Report of the NIST Workshop on Digital Signature Certificate Management, December 10-11, 1992
NISTIR 5232	Report of the NSF/NIST Workshop on NSFNET/NREN Security, July 6-7, 1992
NISTIR 5153	Minimum Security Requirements for Multi-User Operating Systems
NISTIR 4976	Assessing Federal and Commercial Information Security Needs
NISTIR 4939	Threat Assessment of Malicious Code and External Attacks
NISTIR 4774	A Review of U.S. and European Security Evaluation Criteria
NISTIR 4749	Sample Statements of Work for Federal Computer Security Services: For use In-House or Contracting Out
NISTIR 4734	Foundations of a Security Policy for use of the National Research and Educational Network
July 2001	A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2
October 2000	An Overview Of The Common Criteria Evaluation And Validation Scheme
July 2000	Identifying Critical Patches With ICat
June 2000	Mitigating Emerging Hacker Threats
December 1999	Operating System Security: Adding to the Arsenal of Security Techniques
November 1999	Acquiring and Deploying Intrusion Detection Systems
September 1999	Securing Web Servers

(continued on next page)

HISTORICAL ARCHIVES CONTINUED

August 1999	The Advanced Encryption Standard: A Status Report
May 1999	Computer Attacks: What They Are and How to Defend Against Them
February 1999	Enhancements to Data Encryption and Digital Signature Federal Standards
January 1999	Secure Web-Based Access to High Performance Computing Resources
November 1998	Common Criteria: Launching the International Standard
September 1998	Cryptography Standards and Infrastructures for the Twenty-First Century
June 1998	Training for Information Technology Security: Evaluating the Effectiveness of Results-Based Learning
April 1998	Training Requirements for Information Technology Security: An Introduction to Results-Based Learning
March 1998	Management of Risks in Information Systems: Practices of Successful Organizations
February 1998	Information Security and the World Wide Web (WWW)
November 1997	Internet Electronic Mail
July 1997	Public Key Infrastructure Technology
April 1997	Security Considerations In Computer Support And Operations
March 1997	Audit Trails
February 1997	Advanced Encryption Standard
January 1997	Security Issues for Telecommuting
October 1996	Generally Accepted System Security Principles (GSSPs): Guidance On Securing Information Technology (IT) Systems
August 1996	Implementation Issues for Cryptography
June 1996	Information Security Policies For Changing Information Technology Environments
May 1996	The World Wide Web: Managing Security Risks
February 1996	Human/Computer Interface Security Issue
September 1995	Preparing for Contingencies and Disasters
August 1995	FIPS 140-1: A Framework for Cryptographic Standards
February 1995	The Data Encryption Standard: An Update
November 1994	Digital Signature Standard
May 1994	Reducing the Risks of Internet Connection and Use
March 1994	Threats to Computer Systems: An Overview
January 1994	Computer Security Policy
November 1993	People: An Important Asset in Computer Security
August 1993	Security Program Management
July 1993	Connecting to the Internet: Security Considerations
May 1993	Security Issues in Public Access Systems
November 1992	Sensitivity of Information
October 1992	Disposition of Sensitive Automated Information
February 1992	Establishing a Computer Security Incident Handling Capability
November 1991	Advanced Authentication Technology
February 1991	Computer Security Roles of NIST and NSA
August 1990	Computer Virus Attacks

Families

The Family categories are identical to the control families found in FIPS 200, SP 800-53, and other related documents. These Family lists mirror the document crosswalk from SP 800-53, Revision 1.

ACCESS CONTROL

FIPS 201-1	Personal Identity Verification for Federal Employees and Contractors
FIPS 200	Security Controls for Federal Information Systems
FIPS 188	Standard Security Labels for Information Transfer
SP 800-100	Information Security Handbook for Managers
SP 800-97	Guide to IEEE 802.11i: Robust Security Networks
SP 800-96	PIV Card / Reader Interoperability Guidelines
SP 800-87	Codes for the Identification of Federal and Federally Assisted Organizations
SP 800-83	Guide to Malware Incident Prevention and Handling
SP 800-81	Secure Domain Name System (DNS) Deployment Guide
SP 800-78	Cryptographic Algorithms and Key Sizes for Personal Identity Verification
SP 800-77	Guide to IPSec VPNs
SP 800-76	Biometric Data Specification for Personal Identity Verification
SP 800-73 Rev 1	Integrated Circuit Card for Personal Identification Verification
SP 800-68	Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist
SP 800-66	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
SP 800-58	Security Considerations for Voice Over IP Systems
SP 800-57	Recommendation on Key Management
SP 800-48	Wireless Network Security: 802.11, Bluetooth, and Handheld Devices
SP 800-46	Security for Telecommuting and Broadband Communications
SP 800-45	Guidelines on Electronic Mail Security
SP 800-44	Guidelines on Securing Public Web Servers
SP 800-43	Systems Administration Guidance for Securing Microsoft Windows 2000 Professional System
SP 800-41	Guidelines on Firewalls and Firewall Policy
SP 800-36	Guide to Selecting Information Technology Security Products
SP 800-28	Guidelines on Active Content and Mobile Code
SP 800-24	PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does
SP 800-19	Mobile Agent Security
SP 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems
SP 800-12	An Introduction to Computer Security: The NIST Handbook

AWARENESS & TRAINING

FIPS 200	Security Controls for Federal Information Systems
SP 800-100	Information Security Handbook for Managers
SP 800-66	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
SP 800-50	Building an Information Technology Security Awareness and Training Program
SP 800-40	Procedures for Handling Security Patches
SP 800-31	Intrusion Detection Systems (IDSs)
SP 800-16	Information Technology Security Training Requirements: A Role- and Performance-Based Model
SP 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems
SP 800-12	An Introduction to Computer Security: The NIST Handbook

AUDIT & ACCOUNTABILITY

FIPS 200	Security Controls for Federal Information Systems
FIPS 198	The Keyed-Hash Message Authentication Code (HMAC)
SP 800-100	Information Security Handbook for Managers
SP 800-92	Guide to Computer Security Log Management
SP 800-89	Recommendation for Obtaining Assurances for Digital Signature Applications
SP 800-86	Guide to Integrating Forensic Techniques into Incident Response
SP 800-83	Guide to Malware Incident Prevention and Handling
SP 800-72	Guidelines on PDA Forensics
SP 800-68	Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist
SP 800-66	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
SP 800-57	Recommendation on Key Management
SP 800-52	Guidelines on the Selection and Use of Transport Layer Security
SP 800-49	Federal S/MIME V3 Client Profile
SP 800-45	Guidelines on Electronic Mail Security
SP 800-44	Guidelines on Securing Public Web Servers
SP 800-42	Guideline on Network Security Testing
SP 800-19	Mobile Agent Security
SP 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems
SP 800-12	An Introduction to Computer Security: The NIST Handbook

CERTIFICATION, ACCREDITATION & SECURITY ASSESSMENTS

FIPS 200	Security Controls for Federal Information Systems
SP 800-100	Information Security Handbook for Managers
SP 800-85	PIV Middleware and PIV Card Application Conformance Test Guidelines
SP 800-79	Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations

(continued on next page)

CERTIFICATION, ACCREDITATION & SECURITY ASSESSMENTS CONTINUED

SP 800-76	Biometric Data Specification for Personal Identity Verification
SP 800-66	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
SP 800-65	Integrating Security into the Capital Planning and Investment Control Process
SP 800-55	Security Metrics Guide for Information Technology Systems
SP 800-53A	Guide for Assessing the Security Controls in Federal Information Systems
SP 800-47	Security Guide for Interconnecting Information Technology Systems
SP 800-42	Guideline on Network Security Testing
SP 800-37	Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems
SP 800-36	Guide to Selecting Information Technology Security Products
SP 800-35	Guide to Information Technology Security Services
SP 800-30	Risk Management Guide for Information Technology Systems
SP 800-26	Security Self-Assessment Guide for Information Technology Systems
SP 800-23	Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
SP 800-22	A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications
SP 800-20	Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures
SP 800-18	Guide for Developing Security Plans for Information Technology Systems
SP 800-17	Modes of Operation Validation System (MOVS): Requirements and Procedures
SP 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems
SP 800-12	An Introduction to Computer Security: The NIST Handbook

CONFIGURATION MANAGEMENT

FIPS 200	Security Controls for Federal Information Systems
SP 800-100	Information Security Handbook for Managers
SP 800-86	Guide to Integrating Forensic Techniques into Incident Response
SP 800-83	Guide to Malware Incident Prevention and Handling
SP 800-81	Secure Domain Name System (DNS) Deployment Guide
SP 800-70	Security Configuration Checklists Program for IT Products
SP 800-68	Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist
SP 800-48	Wireless Network Security: 802.11, Bluetooth, and Handheld Devices
SP 800-46	Security for Telecommuting and Broadband Communications
SP 800-45	Guidelines on Electronic Mail Security
SP 800-44	Guidelines on Securing Public Web Servers
SP 800-43	Systems Administration Guidance for Securing Microsoft Windows 2000 Professional System
SP 800-40	Procedures for Handling Security Patches
SP 800-37	Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems
SP 800-35	Guide to Information Technology Security Services
SP 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems
SP 800-12	An Introduction to Computer Security: The NIST Handbook

CONTINGENCY PLANNING

FIPS 200	Security Controls for Federal Information Systems
SP 800-100	Information Security Handbook for Managers
SP 800-86	Guide to Integrating Forensic Techniques into Incident Response
SP 800-83	Guide to Malware Incident Prevention and Handling
SP 800-81	Secure Domain Name System (DNS) Deployment Guide
SP 800-66	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
SP 800-57	Recommendation on Key Management
SP 800-56A	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
SP 800-50	Building an Information Technology Security Awareness and Training Program
SP 800-45	Guidelines on Electronic Mail Security
SP 800-44	Guidelines on Securing Public Web Servers
SP 800-43	Systems Administration Guidance for Securing Microsoft Windows 2000 Professional System
SP 800-41	Guidelines on Firewalls and Firewall Policy
SP 800-34	Contingency Planning Guide for Information Technology Systems
SP 800-25	Federal Agency Use of Public Key Technology for Digital Signatures and Authentication
SP 800-24	PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does
SP 800-21 Rev 1	Guideline for Implementing Cryptography in the Federal Government
SP 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems
SP 800-13	Telecommunications Security Guidelines for Telecommunications Management Network
SP 800-12	An Introduction to Computer Security: The NIST Handbook

IDENTIFICATION AND AUTHENTICATION

FIPS 201-1	Personal Identity Verification for Federal Employees and Contractors
FIPS 200	Security Controls for Federal Information Systems
FIPS 190	Guideline for the Use of Advanced Authentication Technology Alternatives
FIPS 140-2	Security Requirements for Cryptographic Modules
SP 800-100	Information Security Handbook for Managers
SP 800-97	Guide to IEEE 802.11i: Robust Security Networks
SP 800-96	PIV Card / Reader Interoperability Guidelines
SP 800-87	Codes for the Identification of Federal and Federally Assisted Organizations
SP 800-86	Guide to Integrating Forensic Techniques into Incident Response
SP 800-81	Secure Domain Name System (DNS) Deployment Guide
SP 800-78	Cryptographic Algorithms and Key Sizes for Personal Identity Verification
SP 800-77	Guide to IPSec VPNs
SP 800-76	Biometric Data Specification for Personal Identity Verification
SP 800-73 Rev 1	Integrated Circuit Card for Personal Identification Verification
SP 800-72	Guidelines on PDA Forensics

(continued on next page)

IDENTIFICATION AND AUTHENTICATION CONTINUED

SP 800-68	Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist
SP 800-66	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
SP 800-63	Recommendation for Electronic Authentication
SP 800-52	Guidelines on the Selection and Use of Transport Layer Security
SP 800-48	Wireless Network Security: 802.11, Bluetooth, and Handheld Devices
SP 800-46	Security for Telecommuting and Broadband Communications
SP 800-45	Guidelines on Electronic Mail Security
SP 800-44	Guidelines on Securing Public Web Servers
SP 800-36	Guide to Selecting Information Technology Security Products
SP 800-32	Introduction to Public Key Technology and the Federal PKI Infrastructure
SP 800-25	Federal Agency Use of Public Key Technology for Digital Signatures and Authentication
SP 800-24	PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does
SP 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems
SP 800-12	An Introduction to Computer Security: The NIST Handbook

INCIDENT RESPONSE

FIPS 200	Security Controls for Federal Information Systems
SP 800-100	Information Security Handbook for Managers
SP 800-92	Guide to Computer Security Log Management
SP 800-83	Guide to Malware Incident Prevention and Handling
SP 800-66	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
SP 800-61	Computer Security Incident Handling Guide
SP 800-50	Building an Information Technology Security Awareness and Training Program
SP 800-36	Guide to Selecting Information Technology Security Products
SP 800-31	Intrusion Detection Systems (IDSs)
SP 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems
SP 800-12	An Introduction to Computer Security: The NIST Handbook

MAINTENANCE

FIPS 200	Security Controls for Federal Information Systems
SP 800-100	Information Security Handbook for Managers
SP 800-88	Media Sanitization Guide
SP 800-77	Guide to IPSec VPNs
SP 800-34	Contingency Planning Guide for Information Technology Systems
SP 800-24	PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does
SP 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems
SP 800-12	An Introduction to Computer Security: The NIST Handbook

MEDIA PROTECTION

FIPS 200	Security Controls for Federal Information Systems
SP 800-100	Information Security Handbook for Managers
SP 800-92	Guide to Computer Security Log Management
SP 800-88	Media Sanitization Guide
SP 800-86	Guide to Integrating Forensic Techniques into Incident Response
SP 800-72	Guidelines on PDA Forensics
SP 800-66	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
SP 800-57	Recommendation on Key Management
SP 800-36	Guide to Selecting Information Technology Security Products
SP 800-24	PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does
SP 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems
SP 800-12	An Introduction to Computer Security: The NIST Handbook

PHYSICAL & ENVIRONMENTAL PROTECTION

FIPS 200	Security Controls for Federal Information Systems
SP 800-100	Information Security Handbook for Managers
SP 800-96	PIV Card / Reader Interoperability Guidelines
SP 800-92	Guide to Computer Security Log Management
SP 800-86	Guide to Integrating Forensic Techniques into Incident Response
SP 800-78	Cryptographic Algorithms and Key Sizes for Personal Identity Verification
SP 800-76	Biometric Data Specification for Personal Identity Verification
SP 800-73 Rev 1	Integrated Circuit Card for Personal Identification Verification
SP 800-66	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
SP 800-58	Security Considerations for Voice Over IP Systems
SP 800-24	PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does
SP 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems
SP 800-12	An Introduction to Computer Security: The NIST Handbook

PLANNING

FIPS 201-1	Personal Identity Verification for Federal Employees and Contractors
FIPS 200	Security Controls for Federal Information Systems
FIPS 199	Standards for Security Categorization of Federal Information and Information Systems
SP 800-100	Information Security Handbook for Managers
SP 800-89	Recommendation for Obtaining Assurances for Digital Signature Applications
SP 800-81	Secure Domain Name System (DNS) Deployment Guide

(continued on next page)

PLANNING CONTINUED

SP 800-66	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
SP 800-65	Integrating Security into the Capital Planning and Investment Control Process
SP 800-64	Security Considerations in the Information System Development Life Cycle
SP 800-58	Security Considerations for Voice Over IP Systems
SP 800-57	Recommendation on Key Management
SP 800-48	Wireless Network Security: 802.11, Bluetooth, and Handheld Devices
SP 800-46	Security for Telecommuting and Broadband Communications
SP 800-45	Guidelines on Electronic Mail Security
SP 800-44	Guidelines on Securing Public Web Servers
SP 800-42	Guideline on Network Security Testing
SP 800-41	Guidelines on Firewalls and Firewall Policy
SP 800-40, Ver 2	Creating a Patch and Vulnerability Management Program
SP 800-40	Procedures for Handling Security Patches
SP 800-37	Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems
SP 800-34	Contingency Planning Guide for Information Technology Systems
SP 800-33	Underlying Technical Models for Information Technology Security
SP 800-32	Introduction to Public Key Technology and the Federal PKI Infrastructure
SP 800-31	Intrusion Detection Systems (IDSs)
SP 800-30	Risk Management Guide for Information Technology Systems
SP 800-27	Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
SP 800-26	Security Self-Assessment Guide for Information Technology Systems
SP 800-25	Federal Agency Use of Public Key Technology for Digital Signatures and Authentication
SP 800-21 Rev 1	Guideline for Implementing Cryptography in the Federal Government
SP 800-19	Mobile Agent Security
SP 800-18	Guide for Developing Security Plans for Information Technology Systems
SP 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems
SP 800-12	An Introduction to Computer Security: The NIST Handbook

PERSONNEL SECURITY

FIPS 200	Security Controls for Federal Information Systems
SP 800-100	Information Security Handbook for Managers
SP 800-66	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
SP 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems
SP 800-12	An Introduction to Computer Security: The NIST Handbook

RISK ASSESSMENT

FIPS 200	Security Controls for Federal Information Systems
FIPS 199	Standards for Security Categorization of Federal Information and Information Systems
SP 800-100	Information Security Handbook for Managers
SP 800-83	Guide to Malware Incident Prevention and Handling
SP 800-66	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
SP 800-65	Integrating Security into the Capital Planning and Investment Control Process
SP 800-63	Recommendation for Electronic Authentication
SP 800-60	Guide for Mapping Types of Information and Information Systems to Security Categories
SP 800-59	Guideline for Identifying an Information System as a National Security System
SP 800-53A	Guide for Assessing the Security Controls in Federal Information Systems
SP 800-51	Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme
SP 800-48	Wireless Network Security: 802.11, Bluetooth, and Handheld Devices
SP 800-46	Security for Telecommuting and Broadband Communications
SP 800-45	Guidelines on Electronic Mail Security
SP 800-44	Guidelines on Securing Public Web Servers
SP 800-42	Guideline on Network Security Testing
SP 800-40, Ver 2	Creating a Patch and Vulnerability Management Program
SP 800-40	Procedures for Handling Security Patches
SP 800-37	Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems
SP 800-36	Guide to Selecting Information Technology Security Products
SP 800-34	Contingency Planning Guide for Information Technology Systems
SP 800-32	Introduction to Public Key Technology and the Federal PKI Infrastructure
SP 800-31	Intrusion Detection Systems (IDSs)
SP 800-30	Risk Management Guide for Information Technology Systems
SP 800-28	Guidelines on Active Content and Mobile Code
SP 800-26	Security Self-Assessment Guide for Information Technology Systems
SP 800-25	Federal Agency Use of Public Key Technology for Digital Signatures and Authentication
SP 800-24	PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does
SP 800-23	Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
SP 800-19	Mobile Agent Security
SP 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems
SP 800-13	Telecommunications Security Guidelines for Telecommunications Management Network
SP 800-12	An Introduction to Computer Security: The NIST Handbook

SYSTEM & SERVICES ACQUISITION

FIPS 200	Security Controls for Federal Information Systems
SP 800-100	Information Security Handbook for Managers
SP 800-97	Guide to IEEE 802.11i: Robust Security Networks
SP 800-85	PIV Middleware and PIV Card Application Conformance Test Guidelines
SP 800-83	Guide to Malware Incident Prevention and Handling
SP 800-76	Biometric Data Specification for Personal Identity Verification
SP 800-66	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
SP 800-65	Integrating Security into the Capital Planning and Investment Control Process
SP 800-64	Security Considerations in the Information System Development Life Cycle
SP 800-36	Guide to Selecting Information Technology Security Products
SP 800-35	Guide to Information Technology Security Services
SP 800-34	Contingency Planning Guide for Information Technology Systems
SP 800-33	Underlying Technical Models for Information Technology Security
SP 800-31	Intrusion Detection Systems (IDSs)
SP 800-30	Risk Management Guide for Information Technology Systems
SP 800-27	Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
SP 800-23	Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
SP 800-21 Rev 1	Guideline for Implementing Cryptography in the Federal Government
SP 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems
SP 800-12	An Introduction to Computer Security: The NIST Handbook

SYSTEM & COMMUNICATION PROTECTION

FIPS 201-1	Personal Identity Verification for Federal Employees and Contractors
FIPS 200	Security Controls for Federal Information Systems
FIPS 198	The Keyed-Hash Message Authentication Code (HMAC)
FIPS 197	Advanced Encryption Standard
FIPS 190	Guideline for the Use of Advanced Authentication Technology Alternatives
FIPS 186-3	Digital Signature Standard (DSS)
FIPS 180-2	Secure Hash Standard (SHS)
FIPS 140-2	Security Requirements for Cryptographic Modules
SP 800-100	Information Security Handbook for Managers
SP 800-97	Guide to IEEE 802.11i: Robust Security Networks
SP 800-90	Recommendation for Random Number Generation Using Deterministic Random Bit Generators
SP 800-89	Recommendation for Obtaining Assurances for Digital Signature Applications

(continued on next page)

SYSTEM & COMMUNICATION PROTECTION CONTINUED

SP 800-83	Guide to Malware Incident Prevention and Handling
SP 800-81	Secure Domain Name System (DNS) Deployment Guide
SP 800-78	Cryptographic Algorithms and Key Sizes for Personal Identity Verification
SP 800-77	Guide to IPSec VPNs
SP 800-73 Rev 1	Integrated Circuit Card for Personal Identification Verification
SP 800-70	Security Configuration Checklists Program for IT Products
SP 800-68	Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist
SP 800-67	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
SP 800-66	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
SP 800-58	Security Considerations for Voice Over IP Systems
SP 800-57	Recommendation on Key Management
SP 800-56A	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
SP 800-52	Guidelines on the Selection and Use of Transport Layer Security
SP 800-49	Federal S/MIME V3 Client Profile
SP 800-46	Security for Telecommuting and Broadband Communications
SP 800-45	Guidelines on Electronic Mail Security
SP 800-44	Guidelines on Securing Public Web Servers
SP 800-41	Guidelines on Firewalls and Firewall Policy
SP 800-38D	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) for Confidentiality and Authentication
SP 800-38C	Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality
SP 800-38B	Recommendation for Block Cipher Modes of Operation: The RMAC Authentication Mode
SP 800-38A	Recommendation for Block Cipher Modes of Operation - Methods and Techniques
SP 800-36	Guide to Selecting Information Technology Security Products
SP 800-32	Introduction to Public Key Technology and the Federal PKI Infrastructure
SP 800-29	A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2
SP 800-28	Guidelines on Active Content and Mobile Code
SP 800-25	Federal Agency Use of Public Key Technology for Digital Signatures and Authentication
SP 800-22	A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications
SP 800-21 Rev 1	Guideline for Implementing Cryptography in the Federal Government
SP 800-20	Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures
SP 800-19	Mobile Agent Security
SP 800-17	Modes of Operation Validation System (MOVS): Requirements and Procedures
SP 800-15	Minimum Interoperability Specification for PKI Components (MISPC), Version 1
SP 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems
SP 800-12	An Introduction to Computer Security: The NIST Handbook

SYSTEM & INFORMATION INTEGRITY

FIPS 200	Security Controls for Federal Information Systems
SP 800-100	Information Security Handbook for Managers
SP 800-92	Guide to Computer Security Log Management
SP 800-86	Guide to Integrating Forensic Techniques into Incident Response
SP 800-85	PIV Middleware and PIV Card Application Conformance Test Guidelines
SP 800-83	Guide to Malware Incident Prevention and Handling
SP 800-66	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
SP 800-61	Computer Security Incident Handling Guide
SP 800-57	Recommendation on Key Management
SP 800-51	Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme
SP 800-48	Wireless Network Security: 802.11, Bluetooth, and Handheld Devices
SP 800-45	Guidelines on Electronic Mail Security
SP 800-44	Guidelines on Securing Public Web Servers
SP 800-43	Systems Administration Guidance for Securing Microsoft Windows 2000 Professional System
SP 800-42	Guideline on Network Security Testing
SP 800-36	Guide to Selecting Information Technology Security Products
SP 800-31	Intrusion Detection Systems (IDSs)
SP 800-28	Guidelines on Active Content and Mobile Code
SP 800-19	Mobile Agent Security
SP 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems
SP 800-12	An Introduction to Computer Security: The NIST Handbook

Legal Requirements

There are certain legal requirements regarding IT security to which Federal agencies must adhere. Many come from legislation, while others come from Presidential Directives or the Office of Budget and Management (OMB) Circulars. Here is a list of the major sources of these requirements with supporting documents from NIST. Some of the documents are a direct result of mandates given to NIST. Others are documents developed in order to give guidance to Federal agencies in how to carry out legal requirements.

Title III of the E-Gov Act of 2002 [Public Law 107-347]

FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002 (FISMA)

Categorization of all information and information systems and minimum information security requirements for each category

FIPS 200	Security Controls for Federal Information Systems
FIPS 199	Standards for Security Categorization of Federal Information and Information Systems
SP 800-70	Security Configuration Checklists Program for IT Products
SP 800-60	Guide for Mapping Types of Information and Information Systems to Security Categories
SP 800-53	Recommended Security Controls for Federal Information Systems
SP 800-53A	Guide for Assessing the Security Controls in Federal Information Systems
SP 800-37	Guide for the Security Certification and Accreditation of Federal Information Systems
SP 800-34	Contingency Planning Guide for Information Technology Systems
SP 800-30	Risk management Guide for Information Technology Systems
SP 800-26 Rev 1	Guide for Information Security Program Assessments and System Reporting Form
SP 800-18 Rev 1	Guide for Developing Security Plans for Information Systems

Identification of an information system as a national security system

SP 800-59	Guide for Identifying an Information System as a National Security System

Detection and handling of information security incidents

SP 800-84	Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
SP 800-61	Computer Security Incident Handling Guide
SP 800-83	Guide to Malware Incident Prevention and Handling
SP 800-86	Guide to Integrating Forensic Techniques into Incident Response
SP 800-51	Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme
December 2005	Preventing And Handling Malware Incidents: How To Protect Information Technology Systems From Malicious Code And Software

Manage security incidents

SP 800-61	Computer Security Incident Handling Guide
SP 800-83	Guide to Malware Incident Prevention and Handling
SP 800-86	Guide to Integrating Forensic Techniques into Incident Response
SP 800-51	Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme

Annual public report on activities undertaken in the previous year

NISTIR 7285	Computer Security Division 2005 Annual Report
NISTIR 7219	Computer Security Division 2004 Annual Report
NISTIR 7111	Computer Security Division 2003 Annual Report

OMB CIRCULAR A-130: MANAGEMENT OF FEDERAL INFORMATION RESOURCES, APPENDIX III: SECURITY OF FEDERAL AUTOMATED INFORMATION RESOURCES

Assess risks

FIPS 199	Standards for Security Categorization of Federal Information and Information Systems

Certify and accredit systems

FIPS 200	Security Controls for Federal Information Systems
SP 800-37	Guide for the Security Certification and Accreditation of Federal Information Systems

Develop contingency plans and procedures

SP 800-34	Contingency Planning Guide for Information Technology Systems
SP 800-46	Security for Telecommuting and Broadband Communications

Manage system configurations and security throughout the system development life cycle

SP 800-64 Rev 1	Security Considerations in the Information System Development Life Cycle
SP 800-70	Security Configuration Checklists Program for IT Products
SP 800-34	Contingency Planning Guide for Information Technology Systems
NISTIR 7316	Assessment of Access Control Systems

Mandates agency-wide information security program development and implementation

SP 800-18, Rev 1	Guide for Developing Security Plans for Information Systems
SP 800-100	Information Security Handbook: A Guide for Managers
SP 800-12	An Introduction to Computer Security: The NIST Handbook

Conduct security awareness training

SP 800-50	Building an Information Technology Security Awareness and Training Program
SP 800-16	Information Technology Security Training Requirements: A Role- and Performance-Based Model
SP 800-46	Security for Telecommuting and Broadband Communications

E-GOVERNMENT ACT OF 2002

[Public Law 107-347]

Mandates NIST development of security standards

FIPS 199	Standards for Security Categorization of Federal Information and Information Systems
FIPS 200	Security Controls for Federal Information Systems

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE-12 (HSPD-12), COMMON IDENTIFICATION STANDARD FOR FEDERAL EMPLOYEES AND CONTRACTORS

Establishes a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors

FIPS 201-1	Personal Identity Verification for Federal Employees and Contractors
SP 800-85B	PIV Data Model Test Guidelines
SP 800-85A	PIV Card Application and Middleware Interface Test Guidelines (SP800-73 compliance)
SP 800-79	Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations
SP 800-78	Cryptographic Algorithms and Key Sizes for Personal Identity Verification
SP 800-76	Biometric Data Specification for Personal Identity Verification
SP 800-73 Rev 1	Integrated Circuit Card for Personal Identification Verification
NISTIR 7337	Personal Identity Verification Demonstration Summary
NISTIR 7284	Personal Identity Verification Card Management Report
January 2006	Testing And Validation Of Personal Identity Verification (PIV) Components And Subsystems For Conformance To Federal Information Processing Standard 201
August 2005	Implementation Of FIPS 201, Personal Identity Verification (PIV) Of Federal Employees And Contractors
March 2005	Personal Identity Verification (PIV) Of Federal Employees And Contractors: Federal Information Processing Standard (FIPS) 201

OMB CIRCULAR A–11: PREPARATION, SUBMISSION, AND EXECUTION OF THE BUDGET

Capital Planning

SP 800-65	Integrating IT Security into the Capital Planning and Investment Control Process

OTHER REQUIREMENTS WITH SUPPORTING DOCUMENTS

Health Insurance Portability and Accountability Act (HIPAA)

For more information about HIPAA requirements, please visit ***www.cms.hhs.gov***.

Assure health information privacy and security

Standardize electronic data interchange in health care transactions

SP 800-66	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act Security Rule

Homeland Security Presidential Directive-7 (HSPD-7), Critical Infrastructure Identification, Prioritization, and Protection

For more information about HSPD-7, please visit ***www.dhs.gov***.

Protect critical infrastructure

FIPS 199	Standards for Security Categorization of Federal Information and Information Systems
FIPS 200	Security Controls for Federal Information Systems
SP 800-18	Guide for Developing Security Plans for Information Technology Systems
SP 800-30	Risk Management Guide for Information Technology Systems
SP 800-37	Guide for Security Certification and Accreditation of Federal Information Systems
SP 800-53	Recommended Security Controls for Federal Information Systems
SP 800-60	Guide for Mapping Types of Information and Information Systems to Security Categories
SP 800-59	Guideline for Identifying an Information System as a National Security System
SP 800-82	Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security

Tanya Brewer, *Editor*

Matthew Scholl, *Editor*

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

February 2007

Disclaimer: Any mention of commercial products is for information only; it does not imply NIST recommendation or endorsement, nor does it imply that the products mentioned are necessarily the best available for the purpose.

Michael James, *Design/Production*

The DesignPond

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

February 2007