Standards Manager Web Standards List

NIST-National Institute of Standards and Technology

Id	Number	Title	Year	Organization	Page
1	800-50 REV.1	Building a Cybersecurity and Privacy Learning Program	2024	NIST	
2	800-52 REV.2	Measurement Guide for Information Security: Volume 1 ù Identifying and Selecting Measures	2024	NIST	
3	800-55 Vol. 1	Measurement Guide for Information Security: Volume 1 ù Identifying and Selecting Measures	2024	NIST	
4	800-55 Vol. 2	Measurement Guide for Information Security: Volume 2 ù Developing an Information Security Measurement Program	2024	NIST	
5	800-60 Rev. 2	Guide for Mapping Types of Information and Systems to Security Categories	2024	NIST	
6	800-61 REV.3	Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile	2024	NIST	
7	800-63-4	Digital Identity Guidelines: Identity Proofing and Enrollment	2024	NIST	
8	800-63A-4	Digital Identity Guidelines: Identity Proofing and Enrollment	2024	NIST	
9	800-63B-4	Digital Identity Guidelines: Authentication and Authenticator Management	2024	NIST	
10	800-63B SUP1	[Supplement 1] Incorporating Syncable Authenticators into NIST SP 800-63B: Digital Identity Guidelines ù Authentication and Lifecycle Management	2024	NIST	
11	800-63C-4	Digital Identity Guidelines: Federation and Assertions	2024	NIST	
12	800-66 REV.2	Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide	2024	NIST	
13	800-73 PART 1	Interfaces for Personal Identity Verification: Part 1 û PIV Card Application Namespace, Data Model and Representation	2024	NIST	
14	800-73 PART 2	Interfaces for Personal Identity Verification: Part 2 û PIV Card Application Card Command Interface	2024	NIST	
15	800-73 PART 3	Interfaces for Personal Identity Verification: Part 3 û PIV Client Application Programming Interface	2024	NIST	
16	800-78-5	Cryptographic Algorithms and Key Sizes for Personal Identity Verification	2024	NIST	
17	800-90C	Recommendation for Random Bit Generator (RBG) Constructions	2024	NIST	
18	800-108 REV.1	Recommendation for Key Derivation Using Pseudorandom Functions	2024	NIST	
19	800-131A REV.3	Transitioning the Use of Cryptographic Algorithms and Key Lengths	2024	NIST	
20	800-161 REV.1	Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations	2024	NIST	
21	800-171 REV.3	Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations	2024	NIST	
22	800-171A REV.3	Assessing Security Requirements for Controlled Unclassified Information	2024	NIST	
23	800-201	NIST Cloud Computing Forensic Reference Architecture	2024	NIST	
24	800-204D	Strategies for the Integration of Software Supply Chain Security in DevSecOps CI/CD Pipelines	2024	NIST	
25	800-218A	Secure Software Development Practices for Generative AI and Dual-Use Foundation Models: An SSDF Community Profile	2024	NIST	
26	800-223	High-Performance Computing Security: Architecture, Threat Analysis, and Security Posture	2024	NIST	
27	800-224	Keyed-Hash Message Authentication Code (HMAC): Specification of HMAC and Recommendations for Message Authentication	2024	NIST	
28	1299	NIST Cybersecurity Framework 2.0: Resource and Overview Guide	2024	NIST	
29	1300	NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide	2024	NIST	
30	1302	NIST Cybersecurity Framework 2.0: Quick-Start Guide for Using the CSF Tiers	2024	NIST	
31	1303	NIST Cybersecurity Framework 2.0: Enterprise Risk Management Quick-Start Guide	2024	NIST	

32	1305	NIST Cybersecurity Framework 2.0: Quick-Start Guide for Cybersecurity Supply Chain Risk Management (C-SCRM)	2024	NIST	
33	1314	NIST Risk Management Framework (RMF) Small Enterprise Quick Start Guide: A Comprehensive, Flexible, Risk-Based Approach to Managing Information Security and Privacy Risk	2024	NIST	
34	1326	NIST Cybersecurity Supply Chain Risk Management: Due Diligence Assessment Quick-Start Guide	2024	NIST	
35	800-229	Fiscal Year 2023 Cybersecurity and Privacy Annual Report	2024	NIST	
36	800-231	Bug Framework (BF): Formalizing Cybersecurity Weaknesses and Vulnerabilities	2024	NIST	
37	800-233	Service Mesh Proxy Models for Cloud-Native Applications	2024	NIST	
38	1800-35	Implementing a Zero Trust Architecture	2024	NIST	
39	1800-36A	Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management: Enhancing Internet Protocol-Based IoT Device and Network Security	2024	NIST	
40	1800-36B	Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management: Enhancing Internet Protocol-Based IoT Device and Network Security	2024	NIST	
41	1800-36C	Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management: Enhancing Internet Protocol-Based IoT Device and Network Security	2024	NIST	
42	1800-36E	Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management: Enhancing Internet Protocol-Based IoT Device and Network Security	2024	NIST	
43	1800-37A	Addressing Visibility Challenges with TLS 1.3 within the Enterprise	2024	NIST	
44	1800-37B	Addressing Visibility Challenges with TLS 1.3 within the Enterprise	2024	NIST	
45	1800-28	Data Confidentiality: Identifying and Protecting Assets Against Data Breaches	2024	NIST	
46	1800-29	Data Confidentiality: Detect, Respond to, and Recover from Data Breaches	2024	NIST	
47	1800-39A	Implementing Data Classification Practices	2023	NIST	
48	1800-38A	Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography	2023	NIST	
49	1800-38B	Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography	2023	NIST	
50	1800-22	Mobile Device Security: Bring Your Own Device (BYOD)	2023	NIST	
51	1288	Federal Cybersecurity Role-Based Training Approaches, Successes, and Challenges	2023	NIST	
52	800-225	Fiscal Year 2022 Cybersecurity and Privacy Annual Report	2023	NIST	
53	800-226	Guidelines for Evaluating Differential Privacy Guarantees	2023	NIST	
54	800-219 REV.1	Automated Secure Configuration Guidance from the macOS Security Compliance Project (mSCP)	2023	NIST	
55	800-221	Enterprise Impact of Information and Communications Technology Risk: Governing and Managing ICT Risk Programs Within an Enterprise Risk Portfolio	2023	NIST	
56	800-221A	Information and Communications Technology (ICT) Risk Outcomes: Integrating ICT Risk Management Programs with the Enterprise Risk Portfolio	2023	NIST	
57	800-207A	A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Cloud Environments	2023	NIST	
58	800-216	Recommendations for Federal Vulnerability Disclosure Guidelines	2023	NIST	
59	800-217	Guidelines for Personal Identity Verification (PIV) Federation	2023	NIST	
60	800-188	De-Identifying Government Datasets: Techniques and Governance	2023	NIST	
61	800-186	Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters	2023	NIST	
62	800-140B REV.1	Cryptographic Module Validation Program (CMVP) Security Policy Requirements: CMVP Validation Authority Updates to ISO/IEC 24759 and ISO/IEC 19790 Annex B	2023	NIST	
63	800-140C REV.2	Cryptographic Module Validation Program (CMVP)-Approved Security Functions: CMVP Validation Authority Updates to ISO/IEC 24759	2023	NIST	
64	800-140D REV.2	Cryptographic Module Validation Program (CMVP)-Approved Sensitive Security Parameter Generation and Establishment Methods: CMVP Validation Authority Updates to ISO/IEC 24759	2023	NIST	

65	800-157 REV.1	Guidelines for Derived Personal Identity Verification (PIV) Credentials	2023	NIST	
66	800-124 REV.2	Guidelines for Managing the Security of Mobile Devices in the Enterprise	2023	NIST	
67	800-92 REV.1	Cybersecurity Log Management Planning Guide	2023	NIST	
68	800-79 REV.3	Guidelines for the Authorization of PIV Card and Derived PIV Credential Issuers	2023	NIST	
69	800-82 REV.3	Guide to Operational Technology (OT) Security	2023	NIST	
70	800-121 REV.2	Guide to Bluetooth Security	2022	NIST	
71	800-53A REV.5	Assessing Security and Privacy Controls in Information Systems and Organizations	2022	NIST	
72	800-40 REV.4	Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology	2022	NIST	
73	800-160 Vol. 1 REV.1	Engineering Trustworthy Secure Systems	2022	NIST	
74	800-172A	Assessing Enhanced Security Requirements for Controlled Unclassified Information	2022	NIST	
75	800-218	Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities	2022	NIST	
76	800-204C	Implementation of DevSecOps for a Microservices-based Application with Service Mesh	2022	NIST	
77	800-220	Fiscal Year 2021 Cybersecurity and Privacy Annual Report	2022	NIST	
78	800-215	Guide to a Secure Enterprise Network Landscape	2022	NIST	
79	1800-10	Protecting Information and System Integrity in Industrial Control System Environments: Cybersecurity for the Manufacturing Sector	2022	NIST	
80	1800-19	Trusted Cloud: Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments	2022	NIST	
81	1800-30	Securing Telehealth Remote Patient Monitoring Ecosystem	2022	NIST	
82	1800-31	Improving Enterprise Patching for General IT Systems: Utilizing Existing Tools and Performing Processes in Better Ways	2022	NIST	
83	1800-32	Securing Distributed Energy Resources: An Example of Industrial Internet of Things Cybersecurity	2022	NIST	
84	1800-33B	5G Cybersecurity	2022	NIST	
85	1800-34	Validating the Integrity of Computing Devices	2022	NIST	
86	1800-27	Securing Property Management Systems	2021	NIST	
87	1800-15	Securing Small-Business and Home Internet of Things (IoT) Devices: Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD)	2021	NIST	
88	1800-13	Mobile Application Single Sign-On: Improving Authentication for Public Safety First Responders	2021	NIST	
89	1271	Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide	2021	NIST	
90	800-204B	Attribute-based Access Control for Microservices-based Applications using a Service Mesh	2021	NIST	
91	800-213	IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements	2021	NIST	
92	800-213A	IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog	2021	NIST	
93	800-214	2020 Cybersecurity and Privacy Annual Report	2021	NIST	
94	800-160 Vol. 2 REV.1	Developing Cyber-Resilient Systems: A Systems Security Engineering Approach	2021	NIST	
95	800-172	Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171	2021	NIST	
96	800-140F REV.1	CMVP Approved Non-Invasive Attack Mitigation Test Metrics: CMVP Validation Authority Updates to ISO/IEC 24759	2021	NIST	
97	800-47 REV.1	Managing the Security of Information Exchanges	2021	NIST	
98	800-53B	Control Baselines for Information Systems and Organizations	2020	NIST	
99	800-53 REV.5	Security and Privacy Controls for Information Systems and Organizations	2020	NIST	
100	800-56C REV.2	Recommendation for Key-Derivation Methods in Key-Establishment Schemes	2020	NIST	

101	800-57 Part 1 Rev. 5	Recommendation for Key Management: Part 1 û General	2020	NIST	
102	800-133 REV.2	Recommendation for Cryptographic Key Generation	2020	NIST	
103	800-137A	Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment	2020	NIST	
104	800-140	FIPS 140-3 Derived Test Requirements (DTR): CMVP Validation Authority Updates to ISO/IEC 24759	2020	NIST	
105	800-140A	CMVP Documentation Requirements: CMVP Validation Authority Updates to ISO/IEC 24759	2020	NIST	
106	800-77 REV.1	Guide to IPsec VPNs	2020	NIST	
107	800-63C	Digital Identity Guidelines: Federation and Assertions	2020	NIST	
108	800-63B	Digital Identity Guidelines: Authentication and Lifecycle Management	2020	NIST	
109	800-63A	Digital Identity Guidelines: Enrollment and Identity Proofing	2020	NIST	
110	800-63-3	Digital Identity Guidelines	2020	NIST	
111	800-140F	CMVP Approved Non-Invasive Attack Mitigation Test Metrics: CMVP Validation Authority Updates to ISO/IEC 24759	2020	NIST	
112	800-140E	CMVP Approved Authentication Mechanisms: CMVP Validation Authority Requirements for ISO/IEC 19790 Annex E and ISO/IEC 24579 Section 6.17	2020	NIST	
113	800-175B REV.1	Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms	2020	NIST	
114	800-208	Recommendation for Stateful Hash-Based Signature Schemes	2020	NIST	
115	800-209	Security Guidelines for Storage Infrastructure	2020	NIST	
116	800-210	General Access Control Guidance for Cloud Systems	2020	NIST	
117	800-211	2019 NIST/ITL Cybersecurity Program Annual Report	2020	NIST	
118	800-204A	Building Secure Microservices-based Applications Using Service-Mesh Architecture	2020	NIST	
119	800-206	Annual Report 2018: NIST/ITL Cybersecurity Program	2020	NIST	
120	800-207	Zero Trust Architecture	2020	NIST	
121	800-181 REV.1	Workforce Framework for Cybersecurity (NICE Framework)	2020	NIST	
122	1500-16	Improving Veteran Transitions to Civilian Cybersecurity Roles: Workshop Report	2020	NIST	
123	1800-11	Data Integrity: Recovering from Ransomware and Other Destructive Events	2020	NIST	
124	1800-16	Securing Web Transactions: TLS Server Certificate Management	2020	NIST	
125	1800-21	Mobile Device Security: Corporate-Owned Personally-Enabled (COPE)	2020	NIST	
126	1800-23	Energy Sector Asset Management: For Electric Utilities, Oil & Gas Industry	2020	NIST	
127	1800-24	Securing Picture Archiving and Communication System (PACS): Cybersecurity for the Healthcare Sector	2020	NIST	
128	1800-25	Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events	2020	NIST	
129	1800-26	Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events	2020	NIST	
130	1800-17	Multifactor Authentication for E-Commerce: Risk-Based, FIDO Universal Second Factor Implementations for Purchasers	2019	NIST	
131	1800-12	Derived Personal Identity Verification (PIV) Credentials	2019	NIST	
132	1800-14	Protecting the Integrity of Internet Routing: Border Gateway Protocol (BGP) Route Origin Validation	2019	NIST	
133	1800-4	Mobile Device Security: Cloud and Hybrid Builds	2019	NIST	
134	1800-7	Situational Awareness for Electric Utilities	2019	NIST	
135	1500-4 REV.2	NIST Big Data Interoperability Framework: Volume 4, Security and Privacy Version 3	2019	NIST	
136	800-177 REV.1	Trustworthy Email	2019	NIST	
137	800-189	Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation	2019	NIST	
138	800-205	Attribute Considerations for Access Control Systems	2019	NIST	
139	800-204	Security Strategies for Microservices-based Application Systems	2019	NIST	

140	800-162	Guide to Attribute Based Access Control (ABAC) Definition and Considerations	2019	NIST	
141	800-163 REV.1	Vetting the Security of Mobile Applications	2019	NIST	
142	800-131A REV.2	Transitioning the Use of Cryptographic Algorithms and Key Lengths	2019	NIST	
143	800-128	Guide for Security-Focused Configuration Management of Information Systems	2019	NIST	
144	800-57 Part 2 REV.1	Recommendation for Key Management: Part 2 û Best Practices for Key Management Organizations	2019	NIST	
145	800-56B REV.2	Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography	2019	NIST	
146	800-38G REV.1	Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption	2019	NIST	
147	800-37 REV.2	Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy	2018	NIST	
148	800-56A REV.3	Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography	2018	NIST	
149	500-325	Fog Computing Conceptual Model	2018	NIST	
150	800-126 REV.3	The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.3	2018	NIST	
151	800-126A	SCAP 1.3 Component Specification Version Updates: An Annex to NIST Special Publication 800-126 Revision 3	2018	NIST	
152	800-125A REV.1	Security Recommendations for Server-based Hypervisor Platforms	2018	NIST	
153	800-116 REV.1	Guidelines for the Use of PIV Credentials in Facility Access	2018	NIST	
154	800-70 REV.4	National Checklist Program for IT Products: Guidelines for Checklist Users and Developers	2018	NIST	
155	800-71	Recommendation for Key Establishment Using Symmetric Block Ciphers	2018	NIST	
156	800-90B	Recommendation for the Entropy Sources Used for Random Bit Generation	2018	NIST	
157	800-87 REV.2	Codes for Identification of Federal and Federally-Assisted Organizations	2018	NIST	
158	800-202	Quick Start Guide for Populating Mobile Test Devices	2018	NIST	
159	800-203	2017 NIST/ITL Cybersecurity Program Annual Report	2018	NIST	
160	800-193	Platform Firmware Resiliency Guidelines	2018	NIST	
161	1800-8	Securing Wireless Infusion Pumps in Healthcare Delivery Organizations	2018	NIST	
162	1800-5	IT Asset Management	2018	NIST	
163	1800-6	Domain Name System-Based Electronic Mail Security	2018	NIST	
164	1800-1	Securing Electronic Health Records on Mobile Devices	2018	NIST	
165	1800-2	Identity and Access Management for Electric Utilities	2018	NIST	
166	800-195	2016 NIST/ITL Cybersecurity Program Annual Report	2017	NIST	
167	800-190	Application Container Security Guide	2017	NIST	
168	800-192	Verification and Test Methods for Access Control Policies/Models	2017	NIST	
169	800-187	Guide to LTE Security	2017	NIST	
170	800-12 REV.1	An Introduction to Information Security	2017	NIST	
171	500-320	Report of the Workshop on Software Measures and Metrics to Reduce Security Vulnerabilities (SwMM-RSV)	2016	NIST	
172	800-154	Guide to Data-Centric System Threat Modeling	2016	NIST	
173	800-46 REV.2	Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security	2016	NIST	
174	800-38B	Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication	2016	NIST	
175	800-38G	Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption	2016	NIST	
176	800-85A-4	PIV Card Application and Middleware Interface Test Guidelines (SP 800-73-4 Compliance)	2016	NIST	
177	800-114 REV.1	User's Guide to Telework and Bring Your Own Device (BYOD) Security	2016	NIST	

178	800-125B	Secure Virtual Network Configuration for Virtual Machine (VM) Protection	2016	NIST	
179	800-178	A Comparison of Attribute Based Access Control (ABAC) Standards for Data Service Applications: Extensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC)	2016	NIST	
180	800-180	NIST Definition of Microservices, Application Containers and System Virtual Machines	2016	NIST	
181	800-182	Computer Security Division 2015 Annual Report	2016	NIST	
182	800-183	Networks of 'Things'	2016	NIST	
183	800-184	Guide for Cybersecurity Event Recovery	2016	NIST	
184	800-185	SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash	2016	NIST	
185	800-166	Derived PIV Application and Data Model Test Guidelines	2016	NIST	
186	800-175A	Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies	2016	NIST	
187	800-156	Representation of PIV Chain-of-Trust for Import and Export	2016	NIST	
188	800-150	Guide to Cyber Threat Information Sharing	2016	NIST	
189	800-152	A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS)	2015	NIST	
190	800-176	Computer Security Division 2014 Annual Report	2015	NIST	
191	800-167	Guide to Application Whitelisting	2015	NIST	
192	800-90A REV.1	Recommendation for Random Number Generation Using Deterministic Random Bit Generators	2015	NIST	
193	800-79-2	Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)	2015	NIST	
194	800-57 Part 3 REV.1	Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance	2015	NIST	
195	500-304	Conformance Testing Methodology Framework for ANSI/NIST-ITL 1-2011 Update: 2013, Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information	2015	NIST	
196	800-88 REV.1	Guidelines for Media Sanitization	2014	NIST	
197	800-101 REV.1	Guidelines on Mobile Device Forensics	2014	NIST	
198	800-168	Approximate Matching: Definition and Terminology	2014	NIST	
199	800-170	Computer Security Division 2013 Annual Report	2014	NIST	
200	800-147B	BIOS Protection Guidelines for Servers	2014	NIST	
201	800-157	Guidelines for Derived Personal Identity Verification (PIV) Credentials	2014	NIST	
202	800-165	Computer Security Division 2012 Annual Report	2013	NIST	
203	800-130	A Framework for Designing Cryptographic Key Management Systems	2013	NIST	
204	800-81-2	Secure Domain Name System (DNS) Deployment Guide	2013	NIST	
205	800-83 REV.1	Guide to Malware Incident Prevention and Handling for Desktops and Laptops	2013	NIST	
206	800-76-2	Biometric Specifications for Personal Identity Verification	2013	NIST	
207	800-61 REV.2	Computer Security Incident Handling Guide	2012	NIST	
208	800-126 REV.2	The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2	2012	NIST	
209	800-107 REV.1	Recommendation for Applications Using Approved Hash Algorithms	2012	NIST	
210	800-38F	Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping	2012	NIST	
211	800-30 REV.1	Guide for Conducting Risk Assessments	2012	NIST	
212	800-153	Guidelines for Securing Wireless Local Area Networks (WLANs)	2012	NIST	
213	800-146	Cloud Computing Synopsis and Recommendations	2012	NIST	
214	800-147	BIOS Protection Guidelines	2011	NIST	
215	800-144	Guidelines on Security and Privacy in Public Cloud Computing	2011	NIST	

216	800-145	The NIST Definition of Cloud Computing	2011	NIST	
217	800-39	Managing Information Security Risk: Organization, Mission, and Information System View	2011	NIST	
218	800-51 REV.1	Guide to Using Vulnerability Naming Schemes	2011	NIST	
219	800-135 REV.1	Recommendation for Existing Application-Specific Key Derivation Functions	2011	NIST	
220	800-137	Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations	2011	NIST	
221	800-126 REV.1	The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.1	2011	NIST	
222	800-125	Guide to Security for Full Virtualization Technologies	2011	NIST	
223	800-132	Recommendation for Password-Based Key Derivation: Part 1: Storage Applications	2010	NIST	
224	800-119	Guidelines for the Secure Deployment of IPv6	2010	NIST	
225	800-122	Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)	2010	NIST	
226	800-34 REV.1	Contingency Planning Guide for Federal Information Systems	2010	NIST	
227	800-38A	Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode	2010	NIST	
228	800-38E	Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality on Storage Devices	2010	NIST	
229	800-142	Practical Combinatorial Testing	2010	NIST	
230	800-41 REV.1	Guidelines on Firewalls and Firewall Policy	2009	NIST	
231	800-102	Recommendation for Digital Signature Timeliness	2009	NIST	
232	800-123	Guide to General Server Security	2008	NIST	
233	800-113	Guide to SSL VPNs	2008	NIST	
234	800-115	Technical Guide to Information Security Testing and Assessment	2008	NIST	
235	800-55 REV.1	Performance Measurement Guide for Information Security	2008	NIST	
236	800-60 Vol. 1 REV.1	Guide for Mapping Types of Information and Information Systems to Security Categories	2008	NIST	
237	800-60 Vol. 2 REV.1	Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices	2008	NIST	
238	800-28 Version 2	Guidelines on Active Content and Mobile Code	2008	NIST	
239	800-44 Version 2	Guidelines on Securing Public Web Servers	2007	NIST	
240	800-45 Version 2	Guidelines on Electronic Mail Security	2007	NIST	
241	800-38C	Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality	2007	NIST	
242	800-38D	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC	2007	NIST	
243	800-111	Guide to Storage Encryption Technologies for End User Devices	2007	NIST	
244	800-94	Guide to Intrusion Detection and Prevention Systems (IDPS)	2007	NIST	
245	800-95	Guide to Secure Web Services	2007	NIST	
246	800-97	Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i	2007	NIST	
247	800-98	Guidelines for Securing Radio Frequency Identification (RFID) Systems	2007	NIST	
248	800-100	Information Security Handbook: A Guide for Managers	2007	NIST	
249	800-96	PIV Card to Reader Interoperability Guidelines	2006	NIST	
250	800-84	Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities	2006	NIST	
251	800-89	Recommendation for Obtaining Assurances for Digital Signature Applications	2006	NIST	
252	800-85B	PIV Data Model Test Guidelines	2006	NIST	
253	800-86	Guide to Integrating Forensic Techniques into Incident Response	2006	NIST	

254	800-92	Guide to Computer Security Log Management	2006	NIST	
255	800-18 REV.1	Guide for Developing Security Plans for Federal Information Systems	2006	NIST	
256	800-58	Security Considerations for Voice Over IP Systems	2005	NIST	
257	800-72	Guidelines on PDA Forensics	2004	NIST	
258	800-59	Guideline for Identifying an Information System as a National Security System	2003	NIST	
259	800-35	Guide to Information Technology Security Services	2003	NIST	
260	800-49	Federal S/MIME V3 Client Profile	2002	NIST	
261	500-189	Security in ISDN	1991	NIST	
262	500-160	Report of the Invitational Workshop on Integrity Policy in Computer Information Systems (WIPCIS)	1989	NIST	
263	500-166	Computer Viruses and Related Threats: a Management Guide	1989	NIST	
264	500-169	Executive Guide to the Protection of Information Resources	1989	NIST	
265	500-170	Management Guide to the Protection of Information Resources	1989	NIST	
266	500-171	Computer Users' Guide to the Protection of Information Resources	1989	NIST	
267	500-174	Guide for Selecting Automated Risk Analysis Tools	1989	NIST	
268	500-153	Guide to Auditing for Controls and Security: A System Development Life Cycle Approach	1988	NIST	
269	500-156	Message Authentication Code (MAC) Validation System: Requirements and Procedures	1988	NIST	
270	500-157	Smart Card Technology: New Methods for Computer Access Control	1988	NIST	
271	500-158	Accuracy, Integrity, and Security in Computerized Vote-Tallying	1988	NIST	
272	500-137	Security for Dial-Up Lines	1986	NIST	
273	500-120	Security of Personal Computer Systems: A Management Guide	1985	NIST	
274	500-133	Technology Assessment: Methods for Measuring the Level of Computer Security	1985	NIST	
275	500-134	Guide on Selecting ADP Backup Process Alternatives	1985	NIST	
276	500-109	Overview of Computer Security Certification and Accreditation	1984	NIST	
277	500-85	Executive Guide to ADP Contingency Planning	1982	NIST	
278	500-57	Audit and Evaluation of Computer Security II: System Vulnerabilities and Controls	1980	NIST	
279	500-61	Maintenance Testing for the Data Encryption Standard	1980	NIST	
280	500-20	Validating the Correctness of Hardware Implementations of the NBS Data Encryption Standard	1980	NIST	
281	500-42	A Survey of Remote Monitoring	1979	NIST	
282	500-54	A Key Notarization System for Computer Networks	1979	NIST	
283	500-21 VOL.1	Design Alternatives for Computer Network Security	1978	NIST	
284	500-21 VOL.2	The Network Security Center: a System Level Approach to Computer Network Security	1978	NIST	
285	500-24	Performance Assurance and Data Integrity Practices	1978	NIST	
286	500-25	An Analysis of Computer Security Safeguards for Detecting and Preventing Intentional Computer Misuse	1978	NIST	
287	500-27	Computer Security and the Data Encryption Standard: Proceedings of the Conference on Computer Security and the Data Encryption Standard	1978	NIST	
288	500-30	Effective Use of Computing Technology in Vote-Tallying	1978	NIST	
289	500-9	The Use of Passwords for Controlled Access to Computer Resources	1977	NIST	
290	500-19	Audit and Evaluation of Computer Security	1977	NIST	
291	404	Approaches to Privacy and Security in Computer Systems: Proceedings of a Conference Held at the National Bureau of Standards March 4-5, 1974	1974	NIST	
292	800-22 REV.1A	Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications		NIST	
293	800-38A-ADD	Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode		NIST	

294	1800-38C	Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography		NIST	