**Cybersecurity Policy Reference**

**12/02/2024**

This reference guide is maintained by the Cybersecurity Policy Team of OCIO to provide contract teams and programs with a current list and location of key cybersecurity documents that may be referred to as an Applicable Documents List (ADL). This reference guide is not an ADL.

While efforts have been made to list the most relevant cybersecurity policies and documents applicable to NASA, the list is not exhaustive. Program officials should make contracting officers aware of any additional standards, specifications, or requirements relevant to execution of a contract.

If you have recommendations for additions to this reference, please email them to agency-cspd-policy@mail.nasa.gov

**General**

**NPRs and NPDs may be found through NODIS:** [**https://nodis3.gsfc.nasa.gov/**](https://nodis3.gsfc.nasa.gov/)**://nodis3.gsfc.nasa.gov**

**Specifications and Standards may be found through NTSS (NASA account required):** [**https://standards.nasa.gov**](https://standards.nasa.gov)

**Note: NASA-SPEC-2600, Enumeration of ASCS Cybersecurity Requirements contains the authoritative list of ASCS technical standards and specifications. Not all ASCS standards and specifications are repeated in the table below. Offerors SHALL comply with all standards and specifications within NASA-SPEC-2600 throughout the life of the contract.**

**ASCS technical standards and specifications may be found through CSET (NASA account required):** [**https://cset.nasa.gov**](https://cset.nasa.gov)

**NASA IT Policy Memoranda may be found a (NASA account required)t:** [**IT-Policy Memoranda (sharepoint.com)**](https://nasa.sharepoint.com/sites/business-management/SitePages/IT-Policy-Memoranda.aspx)

**NASA IT Handbooks may be found through CSET (NASA account required):** [**https://cset.nasa.gov**](https://cset.nasa.gov)

[**NASA Policy Directives (NPD) and NASA Procedural Requirements (NPR)**](https://nodis3.gsfc.nasa.gov/)

|  |  |  |
| --- | --- | --- |
| **Document ID** | **Subject/Title** | **Date** |
| NPR 1382.1B | NASA Privacy Procedural Requirements | July 26, 2022 |
| NPD1382.17K | NASA Privacy Policy | March 28, 2022 |
| NPD 1440.6I | NASA Records Management | September 10, 2014 |
| NPR 1441.1E | NASA Records Management Program Requirements (with updates) | January 29, 2015 |
| NPD 2540.1K | Personal Use of Government Office Equipment Including Information Technology | August 11, 2022 |
| NPD 2800.1E | Managing Information Technology | December 9, 2019 |
| NPD 2810.1F | NASA Information Security Policy | January 21, 2022 |
| NPR 2810.1F | Security of Information and Information Systems | January 03, 2022 |
| NID 2810.142 | Possession and Use of NASA Information and Information Systems Outside of the United States and United States Territories. | December 5, 2023 |
| NPR 2810.7 | Controlled Unclassified Information | October 22, 2021 |
| NPD 2830.1D | NASA Enterprise Architecture | November 17, 2020 |
| NPR 2830.1A | NASA Enterprise Architecture Procedures | December 19, 2013 |
| NPR 2841.1 | Identity, Credential, and Access Management (Revalidated to expire on January 06, 2027.) | January 06, 2011 |
| NPR 7120.7A | NASA Information Technology Program and Project Management Requirements | August 17, 2020 |
| NPR 7150.2D | NASA Software Engineering Requirements | March 8, 2022 |

**NASA Advisory Implementing Instructions (NAII)**

|  |  |  |
| --- | --- | --- |
| **Document ID** | **Subject/Title** | **Date** |
| NAII 2810.1 | Networks in NASA Internet Protocol (IP) Space or NASA Physical Space | June 12, 2020 |
| NAII 2810.2 | Email Services | November 4, 2020 |

**Handbooks and Standard Operating Procedures**

|  |  |  |
| --- | --- | --- |
| **Document ID** | **Subject/Title** | **Date** |
| IT-HBK-1440.01-01 | Records Planning & Management: Records Management & Records Life Cycle - Overview | July 02, 2014 |
| IT-HBK-1441.01-01 | Records Retention and Disposition: Overview | July 02, 2014 |
| IT-HBK-2841.0-03A | Identity, Credential, and Access Management Services (ICAM) | November 02, 2020 |
| ITS-HBK-1382.03-01 | Privacy – Collections, PTAs, and PIAs | March 10, 2022 |
| ITS-HBK-1382.03-02 | Privacy Annual Reporting Procedures: Reviewing and Reducing PII and Unnecessary Use of SSN. | February 16, 2022 |
| ITS-HBK-1382.04-01 | Privacy and Cybersecurity: Supporting an Integrated Controls Framework | February 14, 2023 |
| ITS-HBK-1382.05-01 | Privacy Incident Response and Management: Breach Response Team Checklist | July 19, 2022 |
| ITS-HBK-1382.06-01 | Web Privacy Notices and Redress | July 19, 2022 |
| *ITS-HBK-1382.07-01* | *Privacy Awareness and Training (decision pending on the future this hbk)* | *November 19, 2018* |
| *ITS-HBK-1382.08-01* | *Privacy Accountability (decision pending on the future of this hbk.)* | *November 19, 2018* |
| ITS-HBK-2810.002-1C | Format and Procedures for IT Security Policies and Handbooks | August 11, 2022 |
| ITS-HBK-AASTEP0.v1.0.0 | Step 0: Prepare Policy | June 8, 2023 |
| ITS-HBK-AASTEP1.v1.0.0 | [Step 1: Categorize Policy](https://cset.nasa.gov/wp-content/uploads/2022/01/ITS-HBK-AASTEP1.v1.0.0.pdf) | June 8, 2023 |
| ITS-HBK-AASTEP2.v1.0.0 | [Step 2: Select Policy](https://cset.nasa.gov/wp-content/uploads/2022/01/ITS-HBK-AASTEP2.v1.0.0.pdf) | June 8, 2023 |
| ITS-HBK-AASTEP3.v1.0. | [Step 3: Implement Policy](https://cset.nasa.gov/wp-content/uploads/2022/01/ITS-HBK-AASTEP3.v.1.0.0.pdf) | June 8, 2023 |
| ITS-HBK-AASTEP4.v1.0.0 | [Step 4: Assess Policy](https://cset.nasa.gov/wp-content/uploads/2022/01/ITS-HBK-AASTEP4.v1.0.0-2.pdf) | June 8, 2023 |
| ITS-HBK-AASTEP5.v1.0.0 | [Step 5: Authorize Policy](https://cset.nasa.gov/wp-content/uploads/2022/01/ITS-HBK-AASTEP5.v1.0.0.pdf) | June 8, 2023 |
| ITS-HBK-AASTEP6.v1.0.0 | [Step 6: Monitor Policy](https://cset.nasa.gov/wp-content/uploads/2022/01/ITS-HBK-AASTEP6.v.1.0.0.pdf) | June 8, 2023 |
| ITS-HBK-2810.04-01A | Risk Assessment: Security Categorization, Risk Assessment, Vulnerability Scanning, Expedited Patching | February 27, 2024 |
| ITS-HBK-2810.05-02B | System and Service Acquisition | February 27, 2024 |
| ITS-HBK-2810.06-2B | Cybersecurity and Privacy Awareness, Training and Education | September 20, 2022 |
| ITS-HBK-2810.07-02B | Configuration Management | February 27, 2024 |
| ITS-HBK-2810.08-1A | Contingency Planning | February 27, 2024 |
| *ITS-HBK-2810.09-01* | Incident Response and Management | February 27, 2024 |
| ITS-HBK-2810.09-02A | NASA Information Security Incident Management (CUI) | September 04, 2024 |
| ITS-HBK-2810.09-04 | Incident Response and Management: Guidelines for Data Spillage & Sanitization Procedures | November 03, 2023 |
| ITS-HBK-2810.09-3A | Collection of Electronic Data | November 03, 2023 |
| ITS-HBK-2810.10.02B | Maintenance | February 27, 2024 |
| ITS-HBK-SCRM.2810.v1.2.4 | Supply Chain Risk Management | March 3, 2023 |
| ITS-HBK-2810.11-2B | Media Protection and Sanitization | February 14, 2023 |
| ITS-HBK-2810.12-2B | Physical and Environmental Protection | February 27, 2024 |
| ITS-HBK-2810.13-1B | Personnel Security | February 27, 2024 |
| ITS-HBK-2810.14-03C | System and Information Integrity | February 27, 2024 |
| ITS-HBK-2810.15-1A | Access Control | February 27, 2024 |
| ITS-HBK-2810.15-2A | Access Control: Managed Elevated Privileges | September 06, 2024 |
| ITS-HBK-2810.16-02B | Audit and Accountability | February 27, 2024 |
| ITS-HBK-2810.17-2B | Identification and Authentication | February 27, 2024 |
| ITS-HBK-2810.18-2B | System and Communications Protection | February 27, 2024 |
| ITS-HBK-2810.19-01 | Operational Technology | September 19, 2022 |
| ITS-SOP-2810.03-01A | Review of FMCC POA&Ms and RBDs | April 24, 2023 |
| ITS-SOP-2810.02-02B | Enterprise System Authorization to Operate | April 20, 2023 |
| ITS-SOP-2810-01 | Format and Procedures for IT Security and Policies and Handbooks | July 2022 |

**Standards**

|  |  |  |
| --- | --- | --- |
| **Document ID** | **Subject/Title** | **Date** |
| NASA-SPEC-2600 | Enumeration of ASCS Cybersecurity Requirements | September 22, 2022 |
| NASA-STD-8739.8B | Software Assurance and Software Safety Standard | September 8, 2022 |
| NASA-STD-2804 | Minimum Interoperability Software Suite | December 10, 2020 |
| NASA-STD-2805 | Minimum Hardware Configurations | December 10, 2020 |
| NASA-STD-2603 | Minimum Security and Privacy Requirements for Agency and Center Information System Implementations | October 9, 2019 |
| NASA-STD-2601 | Minimum Cybersecurity Requirements for Computing Systems | June 14, 2023 |
| NASA-STD-2604 | Computing System Configuration Management | August 12, 2019 |
| NASA-STD-2602 | Minimum Information System Owner and End User Security for Data at Rest | April 12, 2023 |

**Memoranda**

|  |  |  |
| --- | --- | --- |
| **Memo Subject** | **From** | **Date** |
| [Use of Software with Automated Reporting Features](https://nasa.sharepoint.com/sites/cio/Signed%20Documents/Forms/AllItems.aspx?id=/sites/cio/Signed%20Documents/Software%20with%20Automated%20Reporting%206_18_2024.pdf&parent=/sites/cio/Signed%20Documents) | NASA CIO | June 18, 2024 |
| Section 508 Compliance and Digital Accessibility | NASA CIO | March 8, 2024 |
| The Importance of Making Digital Content Accessible and Compliance with Section 508 of the Rehabilitation Act | NASA CIO | October 16, 2023 |
| Generative Artificial Intelligence Senior Leader’s Introduction | NASA CIO | May 19, 2023 |
| Transfer of Liability of Phone Numbers to a Different Phone Carrier | NASA CIO | February 13, 2023 |
| Immediate Use of OCOP Performance Management Policy | NASA OCIO | May 5, 2022 |
| Policy document location stability during OCIO transformation | NASA CIO | August 23, 2021 |
| Annual Cybersecurity and Sensitive Unclassified Information Awareness Training | NASA CIO | September 14, 2020 |
| [Your Role in Protecting NASA: Ensuring No Use of Prohibited IT/Telecommunications Services or Equipment at NASA](https://nasa.sharepoint.com/:b:/s/cio/EftUpEsDjqhCkTpFMenc09IBk_-u4Ob5HVeSW9Bylsxx5g?e=cEOY7s) | NASA CIO, OP, OPS | August 26, 2020 |
| [Authorizing Officials and Authorizing Official Designated Representatives](https://nasa.sharepoint.com/:b:/s/cio/EUN4s-1QcUlElf1j3viueOEBOW6J9yC2TldJNuHv7IHh5Q?e=sbFepa) | NASA OCIO | February 27, 2019 |
| Web Site Modernization and Enhanced Security Protocols | NASA Administrator | May 19, 2019 |
| Office of the CIO (OCIO) Reviews of Survey Monkey | NASA Associate Chief information Officer/Senior Agency Information Security Officer | June 7, 2018 |
| Managing Software in Support of NASA's Mission | NASA Administrator (Acting) | May 5, 2017 |
| Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open-Source Software, OCIO Memorandum | NASA CIO | November 7, 2016 |
| NASA Policy Regarding Vulnerability Remediation and POA&M Timeline Standards | Information Technology Management Board (ITMB) | March 4, 2016 |
| Electronic and Information Technology Accessibility | NASA Chief Information Officer | October 10, 2014 |
| NASA Digital Strategy | Associate Administrator for Communications, and Chief Information Officer | March 12, 2014 |
| Implementation of National Institute of Standards and Technology Special Publication 800-53, Revision 4 | Deputy Chief Information Officer for Information Technology Security | December 19, 2013 |
| Rescinding and/or Archiving Information Technology (IT) Security Memoranda | Chief Information Officer | September 20, 2012 |

**Other Documents**

|  |  |  |
| --- | --- | --- |
| **Document ID** | **Subject/Title** | **Date** |
| 40 U.S.C. § 11101 et seq. | Clinger-Cohen Act of 1996 | 1996 |
| National Defense Authorization Act (NDAA) section 889 | Prohibition On Certain Telecommunications and Video Surveillance Services or Equipment | 2019 |
| Executive Order 14028 | Improving the Nation’s Cybersecurity | May 12, 2021 |
| Executive Order 13556 | Controlled Unclassified Information (CUI) | November 4, 2010 |
| Executive Order 13526 | Classified National Security Information, as amended. | December 29, 2009 |
| OMB M-21-07 | IPv6 Implementation | November 19, 2020 |
| OMB M-21-30 | Software Supply Chain Security | August 10, 2021 |
| OMB M-21-31 | Event Security Logging | August 27,2021 |
| OMB M-22-01 | Endpoint Detection and Response | October 8, 2021 |
| OMB M-22-09 | Zero Trust Strategy | January 26, 2022 |
| OMB M-15-13 | Policy to require Secure Connections across Federal Websites and Web Services. | June 8, 2015 |
| OMB M-21-07 | Completing the Transition to Internet Protocol version 6 (IPv6). | November 19, 2020 |
| OMB M-05-24 | Implementation of Homeland Security Directive (HSPD) 12. | August 5, 2005 |
| OMB M-04-04 | E-Authentication Guidance for Federal Agencies. | December 16, 2003 |
| OMB M-06-16 | Protection of Sensitive Agency Information | June 23, 2006 |
| OMB M-00-13 | Privacy Policies and Data Collection on Federal Web Sites. | June 22, 2000 |
| OMB M-01-05 | Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy. | December 20, 2000 |
| OMB M-03-22 | OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002. | September 30, 2003 |
| OMB M-05-08 | Designation of Senior Agency Officials for Privacy. | February 11, 2005 |
| OMB M-10-23 | Guidance for Agency Use of Third-Party Websites and Applications. | June 25, 2010 |
| OMB M-17-12 | Preparing for and Responding to a Breach of Personally Identifiable Information | January 03, 2017 |
| OMB M-02-01 | Guidance for Preparing and Submitting Security Plans of Actions and Milestones. | October 17, 2001 |
| OMB M-06-15 | Safeguarding Personally Identifiable Information, May 22, 2006. | May 22, 2006 |
| OMB M-04-26 | Personal Use Policies and "File Sharing" Technology. | September 8, 2004 |
| OMB M-13-10 | Antideficiency Act Implications of Certain Online Terms of Service Agreements. | April 4, 2013 |
| OMB Circular A-130 | Management of Federal Information Resources. | July 28, 2016 |
| OMB Circular A-108 | Federal Agency Responsibilities for Review, Reporting and Publication under the Privacy Act, December 23, 2016. | December 23, 2016 |
| OMB Circular A-123(Amended with OMB M-16-17) | Management's Responsibility for Enterprise Risk Management and Internal Control, July 15, 2016. | July 15, 2006 |
| OMB Circular A-11 | Preparation, Submission, and Execution of the Budget. | August 15, 2022 |

**FIPS Documents**

|  |  |  |
| --- | --- | --- |
| **Document ID** | **Subject/Title** | **Date** |
| FIPS 202 | SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions | August 8, 2015 |
| FIPS 201-3 | Personal Identity Verification (PIV) of Federal Employees and Contractors | January 1, 2022 |
| FIPS 200 | Minimum Security Requirements for Federal Information and Information Systems | March 1, 2006 |
| FIPS 199 | Standards for Security Categorization of Federal Information and Information Systems | February 1, 2004 |
| FIPS 198-1 | The Keyed-Hash Message Authentication Code (HMAC) | July 16, 2008 |
| FIPS 197 | Advanced Encryption Standard (AES) | November 26, 2001 |
| FIPS 186-4 | Digital Signature Standard (DSS) | July 19, 2013 |
| FIPS 180-4 | Secure Hash Standard (SHS) | August 4, 2015 |
| FIPS 140-3 | Security Requirements for Cryptographic Modules | March 22, 2019 |
| FIPS 140-2 | Security Requirements for Cryptographic Modules | December 3, 2002 |

**NIST Documents**

|  |  |  |
| --- | --- | --- |
| **Document ID** | **Subject/Title** | **Date** |
| SP 1800-10 | Protecting Information and System Integrity in Industrial Control System Environments: Cybersecurity for the Manufacturing Sector | March, 2022 |
| SP 800-220 | Fiscal Year 2021 Cybersecurity and Privacy Annual Report | September, 2022 |
| SP 800-219 Rev. 1 | Automated Secure Configuration Guidance from the macOS Security Compliance Project (mSCP) (Supersedes SP 800-219) | July 2023 |
| SP 800-218 | Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities | February2022 |
| SP 800-213A | IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog | November, 2021 |
| SP 800-213 | IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements | November, 2021 |
| SP 800-210 | General Access Control Guidance for Cloud Systems | July , 2020 |
| SP 800-209 | Security Guidelines for Storage Infrastructure | October, 2020 |
| SP 800-208 | Recommendation for Stateful Hash-Based Signature Schemes | October, 2020 |
| SP 800-207 | Zero Trust Architecture | August , 2020 |
| SP 800-205 | Attribute Considerations for Access Control Systems | June , 2019 |
| SP 800-204C | Implementation of DevSecOps for a Microservices-based Application with Service Mesh | March, 2022 |
| SP 800-204B | Attribute-based Access Control for Microservices-based Applications using a Service Mesh | August, 2021 |
| SP 800-204A | Building Secure Microservices-based Applications Using Service-Mesh Architecture | May, 2020 |
| SP 800-204 | Security Strategies for Microservices-based Application Systems | August, 2019 |
| SP 800-202 | Quick Start Guide for Populating Mobile Test Devices | May, 2018 |
| SP 800-193 | Platform Firmware Resiliency Guidelines | May, 2018 |
| SP 800-192 | Verification and Test Methods for Access Control Policies/Models | June, 2017 |
| SP 800-190 | Application Container Security Guide | September, 2017 |
| SP 800-189 | Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation | December, 2019 |
| SP 800-187 | Guide to LTE Security | December, 2017 |
| SP 800-185 | SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash | December, 2016 |
| SP 800-184 | Guide for Cybersecurity Event Recovery | December, 2016 |
| SP 800-183 | Networks of 'Things' | July, 2016 |
| SP 800-181 Rev. 1 | Workforce Framework for Cybersecurity (NICE Framework) | November, 2020 |
| SP 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) | October, 2016 |
| SP 800-177 Rev. 1 | Trustworthy Email | February, 2019 |
| SP 800-175B Rev. 1 | Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms | March, 2020 |
| SP 800-175A | Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies | August, 2016 |
| SP 800-172A | Assessing Enhanced Security Requirements for Controlled Unclassified Information | March, 2022 |
| SP 800-172 | Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171 | February, 2021 |
| SP 800-171 Rev. 2 | Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations | January, 2021 |
| SP 800-171A | Assessing Security Requirements for Controlled Unclassified Information | June, 2018 |
| SP 800-168 | Approximate Matching: Definition and Terminology | May, 2014 |
| SP 800-167 | Guide to Application Whitelisting | October, 2015 |
| SP 800-166 | Derived PIV Application and Data Model Test Guidelines | June, 2016 |
| SP 800-163 Rev. 1 | Vetting the Security of Mobile Applications | April, 2019 |
| SP 800-162 | Guide to Attribute Based Access Control (ABAC) Definition and Considerations | August, 2019 |
| SP 800-161 Rev. 1 | Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations | May, 2022 |
| SP 800-160 Vol. 2 Rev. 1 | Developing Cyber-Resilient Systems: A Systems Security Engineering Approach | December, 2021 |
| SP 800-160 Vol. 1 Rev. 1 | Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems | November, 2022 |
| SP 800-157 | Guidelines for Derived Personal Identity Verification (PIV) Credentials | December, 2014 |
| SP 800-156 | Representation of PIV Chain-of-Trust for Import and Export | May, 2016 |
| SP 800-153 | Guidelines for Securing Wireless Local Area Networks (WLANs) | February, 2012 |
| SP 800-152 | A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS) | October, 2015 |
| SP 800-150 | Guide to Cyber Threat Information Sharing | October, 2016 |
| SP 800-147B | BIOS Protection Guidelines for Servers | August, 2014 |
| SP 800-147 | BIOS Protection Guidelines | April, 2011 |
| SP 800-146 | Cloud Computing Synopsis and Recommendations | May 29, 2012 |
| SP 800-145 | The NIST Definition of Cloud Computing | September, 2011 |
| SP 800-144 | Guidelines on Security and Privacy in Public Cloud Computing | December, 2011 |
| SP 800-142 | Practical Combinatorial Testing | October, 2010 |
| SP 800-140F | CMVP Approved Non-Invasive Attack Mitigation Test Metrics: CMVP Validation Authority Updates to ISO/IEC 24759 | March, 2020 |
| SP 800-140E | CMVP Approved Authentication Mechanisms: CMVP Validation Authority Requirements for ISO/IEC 19790 Annex E and ISO/IEC 24579 Section 6.17 | March, 2020 |
| SP 800-140D Rev. 2 | CMVP Approved Sensitive Parameter Generation and Establishment Methods: CMVP Validation Authority Updates to ISO/IEC 24759 | July, 2023 |
| SP 800-140C Rev. 2 | CMVP Approved Security Functions: CMVP Validation Authority Updates to ISO/IEC 24759 | July, 2023 |
| SP 800-140B Rev.1 | CMVP Security Policy Requirements: CMVP Validation Authority Updates to ISO/IEC 24759 and ISO/IEC 19790 Annex B | November, 2023 |
| SP 800-140A | CMVP Documentation Requirements: CMVP Validation Authority Updates to ISO/IEC 24759 | March, 2020 |
| SP 800-140 | FIPS 140-3 Derived Test Requirements (DTR): CMVP Validation Authority Updates to ISO/IEC 24759 | March, 2020 |
| SP 800-137A | Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment | May, 2020 |
| SP 800-137 | Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations | September, 2011 |
| SP 800-135 Rev. 1 | Recommendation for Existing Application-Specific Key Derivation Functions | December, 2011 |
| SP 800-133 Rev. 2 | Recommendation for Cryptographic Key Generation | June, 2020 |
| SP 800-132 | Recommendation for Password-Based Key Derivation: Part 1: Storage Applications | December, 2010 |
| SP 800-131A Rev. 2 | Transitioning the Use of Cryptographic Algorithms and Key Lengths | March, 2019 |
| SP 800-130 | A Framework for Designing Cryptographic Key Management Systems | August, 2013 |
| SP 800-128 | Guide for Security-Focused Configuration Management of Information Systems | October, 2019 |
| SP 800-126 Rev. 3 | The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.3 | February, 2018 |
| SP 800-126 Rev. 2 | The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2 | March, 2012 |
| SP 800-126A | SCAP 1.3 Component Specification Version Updates: An Annex to NIST Special Publication 800-126 Revision 3 | February, 2018 |
| SP 800-126 Rev. 1 | The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.1 | February, 2011 |
| SP 800-125B | Secure Virtual Network Configuration for Virtual Machine (VM) Protection | March, 2016 |
| SP 800-125A Rev. 1 | Security Recommendations for Server-based Hypervisor Platforms | June, 2018 |
| SP 800-125 | Guide to Security for Full Virtualization Technologies | January, 2011 |
| SP 800-124 Rev. 1 | Guidelines for Managing the Security of Mobile Devices in the Enterprise | June, 2013 |
| SP 800-123 | Guide to General Server Security | July, 2008 |
| SP 800-122 | Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) | April, 2010 |
| SP 800-121 Rev. 2 | Guide to Bluetooth Security | January, 2022 |
| SP 800-119 | Guidelines for the Secure Deployment of IPv6 | December, 2010 |
| SP 800-116 Rev. 1 | Guidelines for the Use of PIV Credentials in Facility Access | June 29, 2018 |
| SP 800-115 | Technical Guide to Information Security Testing and Assessment | September, 2008 |
| SP 800-114 Rev. 1 | User's Guide to Telework and Bring Your Own Device (BYOD) Security | July, 2016 |
| SP 800-113 | Guide to SSL VPNs | July, 2008 |
| SP 800-111 | Guide to Storage Encryption Technologies for End User Devices | November, 2007 |
| SP 800-108 Rev. 1 | Recommendation for Key Derivation Using Pseudorandom Functions (include updates as of 02-02-24) | August, 2022 |
| SP 800-107 Rev. 1 | Recommendation for Applications Using Approved Hash Algorithms | August, 2012 |
| SP 800-102 | Recommendation for Digital Signature Timeliness | September, 2009 |
| SP 800-101 Rev. 1 | Guidelines on Mobile Device Forensics | May, 2014 |
| SP 800-98 | Guidelines for Securing Radio Frequency Identification (RFID) Systems | April, 2007 |
| SP 800-97 | Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i | February, 2007 |
| SP 800-96 | PIV Card to Reader Interoperability Guidelines | September, 2006 |
| SP 800-95 | Guide to Secure Web Services | August, 2007 |
| SP 800-94 | Guide to Intrusion Detection and Prevention Systems (IDPS) | February, 2007 |
| SP 800-92 | Guide to Computer Security Log Management | September, 2006 |
| SP 800-90B | Recommendation for the Entropy Sources Used for Random Bit Generation | January, 2018 |
| SP 800-90A Rev. 1 | Recommendation for Random Number Generation Using Deterministic Random Bit Generators | June, 2015 |
| SP 800-89 | Recommendation for Obtaining Assurances for Digital Signature Applications | November, 2006 |
| SP 800-88 Rev. 1 | Guidelines for Media Sanitization | December, 2014 |
| SP 800-87 Rev. 2 | Codes for Identification of Federal and Federally-assisted Organizations | April, 2018 |
| SP 800-86 | Guide to Integrating Forensic Techniques into Incident Response | August, 2006 |
| SP 800-85B | PIV Data Model Test Guidelines | July, 2006 |
| SP 800-85A-4 | PIV Card Application and Middleware Interface Test Guidelines (SP 800-73-4 Compliance) | April, 2016 |
| SP 800-84 | Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities | September, 2006 |
| SP 800-83 Rev. 1 | Guide to Malware Incident Prevention and Handling for Desktops and Laptops | July, 2013 |
| SP 800-82 Rev. 3 | Guide to Operational Technology (OT) Security (*superseded SP 800-82 Rev.2 (06-03-2015) Guide to Industrial Control Systems (ICS) Security)* | September, 2023 |
| SP 800-81-2 | Secure Domain Name System (DNS) Deployment Guide | September, 2013 |
| SP 800-79-2 | Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI) | July, 2015 |
| SP 800-78-4 | Cryptographic Algorithms and Key Sizes for Personal Identity Verification | May, 2015 |
| SP 800-77 Rev. 1 | Guide to IPsec VPNs | June, 2020 |
| SP 800-76-2 | Biometric Specifications for Personal Identity Verification | July, 2013 |
| SP 800-73-5 | Interfaces for Personal Identity Verification: Part 1 – PIV Card Application Namespace, Data Model and Representation | July 2024 |
| SP 800-72 | Guidelines on PDA Forensics | November, 2004 |
| SP 800-70 Rev. 4 | National Checklist Program for IT Products: Guidelines for Checklist Users and Developers | February, 2018 |
| SP 800-66 Rev. 2 | An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (superseded SP 800-66 Rev.1) | February, 2024 |
| SP 800-63-3 | Digital Identity Guidelines (include updates up to 03-02-20) | June 2017 |
| SP 800-63C | Digital Identity Guidelines: Federation and Assertions (include updates up to 03-02-20) | June 2017 |
| SP 800-63B | Digital Identity Guidelines: Authentication and Lifecycle Management (include updates up to 03-02-20) | June 2017 |
| SP 800-63A | Digital Identity Guidelines: Enrollment and Identity Proofing (include updates up to 03-02-20) | June 2017 |
| SP 800-61 Rev. 2 | Computer Security Incident Handling Guide | August, 2012 |
| SP 800-60 Vol. 2 Rev. 1 | Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices | August, 2008 |
| SP 800-60 Vol. 1 Rev. 1 | Guide for Mapping Types of Information and Information Systems to Security Categories | August, 2008 |
| SP 800-59 | Guideline for Identifying an Information System as a National Security System | August, 2003 |
| SP 800-58 | Security Considerations for Voice Over IP Systems | January, 2005 |
| SP 800-57 Part 3 Rev. 1 | Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance | January, 2015 |
| SP 800-57 Part 2 Rev. 1 | Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations | May, 2019 |
| SP 800-57 Part 1 Rev. 5 | Recommendation for Key Management: Part 1 – General | May, 2020 |
| SP 800-56C Rev. 2 | Recommendation for Key-Derivation Methods in Key-Establishment Schemes | August, 2020 |
| SP 800-56B Rev. 2 | Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography | March, 2019 |
| SP 800-56A Rev. 3 | Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography | April, 2018 |
| SP 800-55 Rev. 1 | Performance Measurement Guide for Information Security | July, 2008 |
| SP 800-53 Rev. 5 | Security and Privacy Controls for Information Systems and Organizations (include updates up to 09-03-2020) | September, 2020 |
| SP 800-53B | Control Baselines for Information Systems and Organizations (includes updates up to 12-10-2020) | September, 2020 |
| SP 800-53A Rev. 5 | Assessing Security and Privacy Controls in Information Systems and Organizations | January, 2022 |
| SP 800-52 Rev. 2 | Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations | August, 2019 |
| SP 800-51 Rev. 1 | Guide to Using Vulnerability Naming Schemes | February, 2011 |
| SP 800-50 | Building an Information Technology Security Awareness and Training Program | October , 2003 |
| SP 800-49 | Federal S/MIME V3 Client Profile | November, 2002 |
| SP 800-47 Rev. 1 | Managing the Security of Information Exchanges | July, 2021 |
| SP 800-46 Rev. 2 | Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security | July, 2016 |
| SP 800-45 Version 2 | Guidelines on Electronic Mail Security | February, 2007 |
| SP 800-44 Version 2 | Guidelines on Securing Public Web Servers | September, 2007 |
| SP 800-41 Rev. 1 | Guidelines on Firewalls and Firewall Policy | September, 2009 |
| SP 800-40 Rev. 4 | Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology | April, 2022 |
| SP 800-39 | Managing Information Security Risk: Organization, Mission, and Information System View | March, 2011 |
| SP 800-38G | Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption (update August 4, 2016) | March, 2016 |
| SP 800-38F | Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping | December, 2012 |
| SP 800-38E | Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality on Storage Devices | January, 2010 |
| SP 800-38D | Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC | November, 2007 |
| SP 800-38C | Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality (Updated 07-20-2007) | May, 2004 |
| SP 800-38B | Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication (Updated 10-06-2016) | May, 2005 |
| SP 800-38A Addendum | Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode | October, 2010 |
| SP 800-38A | Recommendation for Block Cipher Modes of Operation: Methods and Techniques | December, 2001 |
| SP 800-37 Rev. 2 | Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy | December, 2018 |
| SP 800-35 | Guide to Information Technology Security Services | October, 2003 |
| SP 800-34 Rev. 1 | Contingency Planning Guide for Federal Information Systems | November, 2010 |
| SP 800-30 Rev. 1 | Guide for Conducting Risk Assessments | September, 2012 |
| SP 800-28 Version 2 | Guidelines on Active Content and Mobile Code | March, 2008 |
| SP 800-22 Rev. 1a | A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications | April, 2010 |
| SP 800-18 Rev. 1 | Guide for Developing Security Plans for Federal Information Systems | February, 2006 |
| SP 800-16 | Information Technology Security Training Requirements: A Role- and Performance-Based Model | April,1998 |
| SP 800-12 Rev. 1 | An Introduction to Information Security | June, 2017 |