SECTION J

APPENDIX B

LIST OF APPLICABLE DIRECTIVES

July 2023

In addition to the list of applicable directives referenced below, the contractor shall also comply with supplementary directives (e.g., manuals), which are invoked by a Contractor Requirements Document (CRD) attached to a directive referenced below.

Reference Document	Title	Mod	Effective Date (Contracting Officer Direction Date) and Relevant Notes
5 U.S.C. § 552	Freedom of Information Act (FOIA)		
5 U.S.C. § 552a	Privacy Act of 1974		
29 U.S.C. § 798	Rehabilitation Act		
40 U.S.C. §§ 11101-11704	The Clinger-Cohen Act		
41 U.S.C. Chapter 4	Public Contracts		
42 U.S.C. § 7158	Naval Reactor and Military Application Programs		
44 U.S.C. § 3541 et seq.	Federal Information Security Management Act of 2002 (FISMA)		
50 U.S.C. § 2406	Deputy Administrator for Naval Reactors		
50 U.S.C. § 2511	Naval Nuclear Propulsion Program		
50 U.S.C. § 2401 et seq.	National Nuclear Security Administration (NNSA) Act		
Public Law 100-235	The Computer Security Act of 1987		
Public Law 103–62	The Government Performance and Results Act of 1993		
Public Law 105–277	Government Paperwork Elimination Act		
Public Law 106-229	Electronic Signatures in Global and National Commerce Act (eSignature ACT)		
Public Law 106-65 §3212 (d)	NDAA for FY2000, Title XXXII: NNSA, Subtitle A: Establishment and Organization		
Public Law 107-347	E-Government Act of 2002		
Public Law 111-352	GPRA Modernization Act of 2010		
Public Law 113-187	Federal Records Act		
Public Law 113-283	Federal Information Security Modernization Act of 2014		
Public Law 113-291	The Federal Information Technology Acquisition Reform Act		
Public Law 114-113	Cybersecurity Act of 2015		
Public Law 114-185	FOIA Improvement Act of 2016		
Public Law 114-210	MEGABYTE Act of 2016		
Public Law 115–91	National Defense Authorization Act for Fiscal Year 2018, Subtitle G,		

Reference Document	Title	Mod	Effective Date (Contracting Officer Direction Date) and Relevant Notes
	Modernizing Government Technology (MGT Act)		
Public Law 115-336	The 21st Century IDEA Act		
2 CFR 200.79	Personally Identifiable Information (PII)		
10 CFR Part 1004	Freedom of Information Act (FOIA)		
10 CFR Part 1008	Records Maintained on Individuals (Privacy Act)		
10 CFR § 1017	Identification and Protection of Unclassified Controlled Nuclear Information		
10 CFR § 1045	Nuclear Classification and Declassification		
32 CFR § 2002 et al.	Controlled Unclassified Information		
32 CFR § 2001.23	Classification Marking in the Electronic Environment		
32 CFR 2001.24	Additional Requirements		
36 CFR, Chapter 12, Subchapter B	Records Management		
41 CFR 102-193	Federal Management Regulation - the creation, collection, use, documentation, dissemination, and disposition of records		
48 CFR	Federal Acquisition Regulation		
48 CFR § 4.805	Storage, handling, and contract files		
48 CFR Chapter 9	Department of Energy		
48 CFR § 952.204-2	Security Requirements		
48 CFR § 952.223-71	Integration of Environment Safety, and Health into Work Planning and Execution		
48 CFR § 952.223-72	Radiation Protection and Nuclear Criticality		
48 CFR § 952.223-75	Preservation of Individual Occupational Radiation Exposure Records		
48 CFR § 970.0404	Safeguarding Classified Information		
48 CFR § 970.0407	Contractor Records Retention		
48 CFR § 970.5204-3	Access to and Ownership of Records		
48 CFR § 970.5232-3	Accounts, Records, and Inspection		
Office of Management and Budget (OMB) Circular A-11	Preparation, Submission, and Execution of the Budget		
OMB Circular A-108	Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act		
OMB Circular A-123	Management's Responsibility for Enterprise Risk Management and Internal Control		
OMB Circular A-130	Managing Information as a Strategic Resource		
OMB Memorandum 99-05	Privacy and Personal Information in Federal Records		
OMB Memorandum 99-18	Privacy Policies on Federal Web Sites		
OMB Memorandum 00-13	Privacy Policy and Data Collection on Federal Web Sites		
OMB Memorandum 02-01	Guidance for Preparing, and Submitting Security Plans of Action, and Milestones		
OMB Memorandum 03-22	OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002		
OMB Memorandum 05-04	Policies for Federal Agency Public Websites		
OMB Memorandum 05-08	Designation of Senior Officials for Privacy		
OMB Memorandum 06-15	Safeguarding Personally Identifiable Information		

Reference Document	Title	Mod	Effective Date (Contracting Officer Direction Date) and Relevant Notes
OMB Memorandum 06-19	Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments		
OMB Memorandum 10-27	Information Technology Investment Baseline Management Policy		
OMB Memorandum 11-02	Sharing Data While Protecting Privacy		
OMB Memorandum 12-18	Managing Government Records Directive		
OMB Memorandum 14-03	Enhancing the Security of Federal Information and Information Systems		
OMB Memorandum 15-02	Appendix C to Circular No. A-123, Requirements for Effective Estimation and Remediation of Improper Payments		
OMB Memorandum 15-12	Increasing Transparency of Federal Spending by Making Federal Spending Data Accessible, Searchable, and Reliable		
OMB Memorandum 15-13	Policy to Require Secure Connections across Federal Websites and Web Services		
OMB Memorandum 15-14	Management and Oversight of Federal Information Technology		
OMB Memorandum 16-02	Category Management Policy 15-1: Improving the Acquisition and Management of Common Information Technology: Laptops and Desktops		
OMB Memorandum 16-04	Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government		
OMB Memorandum 16-12	Category Management Policy 16-1: Improving the Acquisition and Management of Common Information Technology: Software Licensing		
OMB Memorandum 16-14, Category Management Policy 16-2	Providing Comprehensive Identity Protection Services, Identity Monitoring, and Data Breach Response		
OMB Memorandum 16-15	Federal Cybersecurity Workforce Strategy		
OMB Memorandum 16-19	Data Center Optimization Initiative (DCOI)		
OMB Memorandum 16-20	Improving the Acquisition and Management of Common IT: Mobile Devices and Services		
OMB Memorandum 16-21	Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open-Source Software		
OMB Memorandum 16-24	Role and Designation of Senior Agency Officials for Privacy		
OMB Memorandum 17-04	Additional Guidance for DATA Act Implementation: Further Requirements for Reporting and Assuring Data Reliability		
OMB Memorandum 17-06	Policies for Federal Agency Public Websites and Digital Services		
OMB Memorandum 17-12	Preparing for and Responding to a Breach of Personally Identifiable Information		
OMB Memorandum 18-12	Implementation of the Modernizing Government Technology Act		
OMB Memorandum 18-16	Appendix A to OMB Circular No. A-123, Management of Reporting and Data Integrity Risk		
OMB Memorandum 19-03	Strengthening the Cybersecurity of Federal Agencies		
OMB Memorandum 19-10	Guidance for Achieving Interoperability with the		

Reference Document	Title	Mod	Effective Date (Contracting Officer Direction Date) and Relevant Notes
	National Freedom of Information Act (FOIA) Portal on FOIA.gov		
OMB Memorandum 19-15	Improving Implementation of the Information Quality Act		
OMB Memorandum 19-16	Centralized Mission Support Capabilities for the Federal Government		
OMB Memorandum 19-17	Enabling Mission Delivery through Improved Identity, Credential, and Access Management		
OMB Memorandum 19-18	Federal Data Strategy – A Framework for Consistency		
OMB Memorandum 19-19	Update to Data Center Optimization Initiative		
OMB Memorandum 19-21	Transition to Electronic Records		
OMB Memorandum 19-26	Update to the Trusted Internet Connections (TIC) Initiative		
OMB Memorandum 20-19	Harnessing Technology to Support Mission Continuity		
OMB Memorandum 20-32	Improving Vulnerability Identification, Management, and Remediation		
OMB Memorandum 21-04	Modernizing Access to and Consent for Disclosure of Records Subject to the Privacy Act		
OMB Memorandum 21-05	Extension of Data Center Optimization Initiative (DCOI)		
OMB Memorandum 21-06	Guidance for Regulation of Artificial Intelligence Applications		
OMB Memorandum 21-07	Completing the Transition to Internet Protocol Version 6 (IPv6)		
OMB Memorandum 21-13	Implementation of Performance Management Statutes		
OMB Memorandum 21-30	Protecting Critical Software Through Enhanced Security Measures		
OMB Memorandum 21-31	Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incident		
OMB Memorandum 22-01	Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response		
OMB Memorandum 22-09	Moving the U.S. Government Toward Zero Trust Cybersecurity Principles		
OMB Memorandum 22-16	Administration Cybersecurity Priorities for the FY 2024 Budget		
OMB Memorandum 22-18	Enhancing the Security of the Software Supply Chain through Secure Software Development Practices		
OMB Memorandum 23-02	Migrating to Post-Quantum Cryptography		
OMB Memorandum 23-03	Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements		
OMB Memorandum 23-07	Update to Transition to Electronic Records		
OMB Memorandum 23-13	No TikTok on Government Devices Implementation Guidance		
OMB Memorandum	Security Authorization of Information Systems in Cloud Computing Environments		
OMB Memorandum	Fiscal Year Guidance on Federal Information		

Reference Document	Title	Mod	Effective Date (Contracting Officer Direction Date) and Relevant Notes
	Security and Privacy Management Requirements (current version)		
Delegation Order No. NA-005.01	Delegation of Authority, Associate Administrator of Information Management and Chief Information Officer		
DOE-DTRA TP 50-2	Procedures for the Use and Control of Logistics Material for Permissive Action Link (PAL) Equipped Weapons (U)		
DOD TB 700-2	DoD Ammunition and Explosives Hazard Classification Procedures		
DOD M 8140.03	Cyberspace Workforce Qualification and Management Program		
DOE O 203.1	Limited Personal Use of Government Office Equipment Including Information Technology		
DOE N 203.1	Software Quality Assurance		
DOE O 130.1A	Budget Planning, Formulation, Execution and Departmental Performance Management		
DOE O 140.1A	Interface with the Defense Nuclear Facilities Safety Board		
DOE O 142.2A Admin Chg 1	Voluntary Offer Safeguards Agreement and Additional Protocol with the International Atomic Energy Agency		
DOE M 142.2-1 Admin Chg 1	Manual for Implementation of the Voluntary Offer Safeguards Agreement and Additional Protocol with the International Atomic Energy Agency		
DOE O 142.3B Chg 1 (LtdChg)	Unclassified Foreign National Access Program		
DOE O 150.1B	Continuity Programs		
DOE O 151.1D Chg 1	Comprehensive Emergency Management System		
DOE O 153.1A	Departmental Nuclear Emergency Support Team Capabilities		
DOE O 200.1A Chg 1 (MinChg)	Information Technology Management		
DOE O 205.1C Chg 1 (LtdChg)	Department of Energy Cybersecurity Program		
DOE O 206.1 Chg1 (MinChg)	Department of Energy Privacy Program		
DOE O 206.2 Chg 1 (LtdChg)	Identity, Credential, and Access Management (ICAM)		
DOE O 210.2A	DOE Corporate Operating Experience Program		
DOE O 221.1B	Reporting Fraud, Waste and Abuse to the Office of Inspector General		
DOE O 221.2A	Cooperation with the Office of Inspector General		
DOE O 225.1B	Accident Investigations		
DOE O 226.1B Chg 1 (Admin Chg)	Implementation of Department of Energy Oversight Policy		
DOE O 227.1A Chg 1 (AdminChg)	Independent Oversight Program		
DOE O 231.1B Admin Chg 1	Environment, Safety and Health Reporting		
DOE O 232.2A Chg 1 (MinChg)	Occurrence Reporting and Processing of Operations Information		
DOE O 241.1B Chg 1 (Admin Chg)	Scientific and Technical Information Management		
DOE O 243.1C	Records Management Program		
DOE O 252.1A Admin Chg 1	Technical Standards Program		

Reference Document	Title	Mod	Effective Date (Contracting Officer Direction Date) and Relevant Notes
DOE O 341.1A	Federal Employee Health Services		
DOE O 410.2 Admin Chg 1	Management of Nuclear Materials		
DOE O 411.2	Scientific Integrity		
DOE O 412.1A Chg1 (AdminChg)	Work Authorization System		
DOE O 413.3B Chg 7 (LtdChg)	Program and Project Management for the Acquisition of Capital Assets		
DOE O 414.1D Chg 2 (LtdChg)	Quality Assurance		
DOE O 415.1 Chg 2 (MinChg)	Information Technology Project Management		
DOE O 420.1C Chg 3 (LtdChg)	Facility Safety		
DOE G 420.1-1A	Nonreactor Nuclear Safety Design Guide for use with DOE O 420.1C, Facility Safety		
DOE O 422.1 Chg 4	Conduct of Operations		
DOE O 425.1D Chg 2 (MinChg)	Verification of Readiness to Start Up or Restart Nuclear Facilities		
DOE O 426.2 Chg 1 (Admin Chg)	Personnel Selection, Training, Qualification and Certification Requirements for DOE Nuclear Facilities		
DOE O 433.1B Chg 1 (Admin Chg)	Maintenance Management Program for DOE Nuclear Facilities		
DOE O 435.1 Chg 2 (AdminChg)	Radioactive Waste Management		
DOE M 435.1-1 Admin Chg 3 (LtdChg)	Radioactive Waste Management Manual		
DOE N 435.1	Contact-Handled and Remote-Handled Transuranic Waste Packaging		
DOE O 436.1A	Departmental Sustainability		
DOE O 440.2C Chg 3 (LtdChg)	Aviation Management and Safety		
DOE M 441.1-1 Chg 1 (Admin Chg)	Nuclear Material Packaging Manual		
DOE O 442.1B	Department of Energy Employee Concerns Program		
DOE O 442.2 Chg 1	Differing Professional Opinions for Technical Issues Involving Environmental, Safety, and Health Technical Concerns		
DOE O 443.1C	Protection of Human Research Subjects		
DOE O 452.1F	Nuclear Explosive and Weapon Surety Program		
DOE O 452.2F	Nuclear Explosive Safety		
DOE O 452.3	Management of the Department of Energy Nuclear Weapons Complex		
DOE O 452.4C	Security and Use Control of Nuclear Explosives and Nuclear Weapons		
DOE O 452.6A Chg 1 (AdminChg)	Nuclear Weapon Surety Interface with the Department of Defense		
DOE O 452.7 Chg 1 (AdminChg)	Protection of Use Control Vulnerabilities and Designs		
DOE O 452.8	Control of Nuclear Weapon Data		
DOE O 457.1A	Nuclear Counterterrorism		
DOE O 458.1 Chg 4 (LtdChg)	Radiation Protection of the Public and the Environment		
DOE O 460.1D Chg 1 (LtdChg)	Hazardous Materials Packaging and Transportation		

Reference Document	Title	Mod	Effective Date (Contracting Officer Direction Date) and Relevant Notes
	Safety		
DOE O 460.2B	Departmental Materials Transportation Management		
DOE O 461.1C Chg 1 (MinChg)	Packaging and Transportation for Offsite Shipment of Materials of National Security Interest		
DOE O 461.2	Onsite Packaging and Transfer of Materials of National Security Interest		
DOE O 462.1 Admin Chg 1	Import and Export of Category 1 and 2 Radioactive Sources and Aggregated Quantities		
DOE O 470.3C Chg 1 (LtdChg)	Design Basis Threat (DBT) Order		
DOE O 470.4B Chg 3 (LtdChg)	Safeguards and Security Program		
DOE O 470.5	Insider Threat Program		
DOE O 470.6 Chg 1 (MinChg)	Technical Security Program		
NNSA SD 470.6	Technical Security Program (OUO)		
DOE O 471.1B	Identification and Protection of Unclassified Controlled Nuclear Information		
DOE O 471.5	Special Access Programs		
DOE O 471.6 Chg 3 (Admin Chg)	Information Security		
DOE O 471.7	Controlled Unclassified Information		
DOE O 472.2A	Personnel Security		
DOE O 473.1A	Physical Protection Program		
DOE O 474.2A	Nuclear Material Control and Accountability		
DOE O 475.1	Counterintelligence Program		
DOE O 475.2B	Identifying Classified Information		
DOE O 483.1B Chg 2 (LtdChg)	DOE Cooperative Research and Development Agreements		
DOE O 484.1 Chg3 (LtdChg)	Reimbursable Work for the Department of Homeland Security		
DOE O 486.1A	Foreign Government Sponsored or Affiliated Activities		
DOE O 520.1B Chg 1 (LtdChg)	Financial Management and Chief Financial Officer Responsibilities		
DOE O 522.1A	Pricing of Departmental Materials and Services		
DOE O 550.1 Chg 1 (LtdChg)	Official Travel		
DOE O 5639.8A	Security of Foreign Intelligence Information and Sensitive Compartmented Information Facilities		
DOE-STD-1020-2016	DOE Standard – Natural Phenomena Hazards Analysis and Design Criteria for DOE Facilities		
DOE-STD-1070-1994 (Reaffirmed July 2014)	DOE Standard – Guidelines for Evaluation of Nuclear Facility Training Programs		
DOE-STD-1073-2016	DOE Standard – Configuration Management		
DOE-STD-1189-2016	DOE Standard – Integration of Safety into the Design Process		
DOE-STD-1212-2019	DOE Standard – Explosives Safety		
DOE-STD-3007-2017	DOE Standard –Preparing Criticality Safety Evaluations at Department of Energy Nonreactor Nuclear Facilities		
DOE-STD-3009-2014	DOE Standard – Preparation of Nonreactor Nuclear Facility Documented Safety Analysis		

Reference Document	Title	Mod	Effective Date (Contracting Officer Direction Date) and Relevant Notes
DOE-STD-3013-2018	Stabilization, Packaging and Storage of Plutonium-Bearing Materials		
DOE-NA-STD-3016-2018	DOE Limited Standard – Hazard Analysis Reports for Nuclear Explosive Operations		
EP-401075 Issue E	Electrical Testers for Nuclear Explosives		
Executive Order 12333	U. S. Intelligence Activities		
Executive Order 12344	Naval Nuclear Propulsion Program		
Executive Order 12656	Assignment of Emergency Preparedness Responsibilities		
Executive Order 13011	Federal Information Technology		
Executive Order 13526	Classified National Security Information		
Executive Order 13556	Controlled Unclassified Information		
Executive Order 13800	Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure		
Executive Order 13587	Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information		
Executive Order 13833	Enhancing the Effectiveness of Agency Chief Information Officers (CIOs)		
Executive Order 14028	Improving the Nation's Cybersecurity		
Joint DOE/DoD Technical Publication 45-51B	Transportation of Nuclear Weapons Material		
National Archives and Records Administration (NARA)	AC 01.2020 Memorandum to Federal Agency Contacts: Annual Move of Permanent Records		
National Archives and Records Administration (NARA)	Archives and Records Center Information System (ARCIS)		
NARA Bulletin 2008-06	Records Storage Facility Standards		
NARA Bulletin 2014-04	Revised Format Guidance for the Transfer of Permanent Electronic Records		
NARA Bulletin 2015-04	Metadata Guidance for the Transfer of Permanent Electronic Records		
National Archives and Records Administration (NARA)	NARA Electronic Records Archives (ERA)		
National Archives and Records Administration (NARA)	NARA Federal Records Management		
NARA publication	Essential Records Guide		
NARA publication	Guidance for Coordinating the Evaluation of Capital Planning and Investment Control (CPIC) Proposals for ERM Applications		

Reference Document	Title	Mod	Effective Date (Contracting Officer Direction Date) and Relevant Notes
National Archives and Records Administration (NARA)	NARA Universal Electronic Records Management (UERM) Requirements		
National Archives and Records Administration (NARA)	National Archives (NA) 14130 Classified Transfer Checklist		
NFPA Codes and Standards	NFPA Codes and Standards		
NHPA CRMP (April 2004)	Pantex Plant Cultural Resource Management Plan		
NNSA Policy Letter: NAP 121.1A	Enterprise-Wide Strategic Planning		
NNSA Policy Letter: NAP 476.1 Admin Chg 1 (formerly NAP-23 Admin Chg 1)	Atomic Energy Act Control of Import and Export Activities		
NNSA Policy Letter: NAP 520.1 Admin Chg 1 (formerly NAP-25 Admin Chg 1)	Management and Operating Contractor Business Meals and Light Refreshments		
NNSA Policy Letter: NAP 540.2 (formerly NAP-31)	NNSA M&O Off-Site Extended Duty Assignments		
NNSA Policy Letter: NAP-220.1	Internal Affairs Program		
NNSA Policy Letter: NAP 401.1A Admin Chg 2	Weapon Quality Policy		
NNSA Policy Letter: NAP-412.1	Financial Integration		
NNSA Policy Letter: NAP-413.1	Data Collection for Cost Estimating		
NNSA Policy Letter: NAP-476.1 Admin Chg 1	Atomic Energy Act Control of Import and Export Activities		
NNSA Policy Letter: NAP 530.1	Cost Allocation Optimization		
NPO Procedure – NPO-SD 3.4.3 (Applies to Pantex Only)	Conducting Readiness Reviews of Hazardous Non-Nuclear Facilities and Activities		
NNSA Quality Plan 100-1 Amendment 4	Application of Quality Requirements to UK and US Procurement Contracts and Loan Authorizations for Research, Design & Development		
NNSA Supplemental Directive – NNSA SD 205.1	Baseline Cybersecurity Program		
Office of the Director of National Intelligence (ODNI), Intelligence Community (IC) Directives (ICD) and IC Policy Guidance (ICPG)	All – implement as directed by The DOE Office of Intelligence and Counterintelligence (IN), as approved for operation of Sensitive Compartmented Information (SCI) systems		
Committee on National Security Systems (CNSS) Instructions, Policies, Directives, and Issuances	Implement as published		
CNSS Policy 1	National Policy for Safeguarding and Control of COMSEC Materials		
CNSS Policy 18	National Policy for Classified Information Spillage		
CNSS Policy 22	Cybersecurity Risk Management Policy		
CNSS Policy 25	National Policy for Public Key Infrastructure in National Security Systems		
CNSS Policy 26	National Policy on Reducing the Risk of Removable Media for National Security Systems		
CNSS Instruction 1001	National Instruction on Classified Information Spillage		
CNSS Instruction 1010	Cyber Incident Response		

Reference Document	Title	Mod	Effective Date (Contracting Officer Direction Date) and Relevant Notes
CNSS Instruction 1253	Security Categorization and Control Selection for National Security		
CNSS Instruction 4004.1	Destruction and Emergency Protection Procedures for COMSEC and Classified Material		
CNSS Instruction 4009	CNSS Glossary		
National Security Agency (NSA)/Central Security Service (CSS) Policy Manual 9-12	Storage Device Sanitization and Destruction Manual		
National Security Directive 42	National Policy for the Security of National Security Telecommunications and Information Systems		
National Security Memorandum 5	Improving Cybersecurity for Critical Infrastructure Control Systems		
National Security Memorandum 8	Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems		
National Security Memorandum 10	Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems		
National Security Presidential Directive 28	United States Nuclear Weapons Command and Control, Safety, and Security		
Presidential Policy Directive (PPD)-21	Critical Infrastructure Security and Resilience		
Presidential Policy Directive (PPD) 41	Federal Government Coordination Architecture for Significant Cyber Incidents		
The White House	2023 National Cybersecurity Strategy		
National Institute of Standards and Technology -- Federal Information Processing Standard 197	Advanced Encryption Standard (AES)		
National Institute of Standards and Technology -- Federal Information Processing Standard 186-4 and 186-5	Digital Signature Standard (DSS)		
National Institute of Standards and Technology -- Federal Information Processing Standard 180-4	Secure Hash Standard (SHS)		
National Institute of Standards and Technology -- Federal Information Processing Standard 140-2 and 140-3	Security Requirements for Cryptographic Modules		
National Institute of Standards and Technology – Interagency Report 7622	Notional Supply Chain Risk Management Practices for Federal Information Systems		
National Institute of Standards and Technology (NIST)	NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework)		
National Institute of Standards and Technology (NIST)	NIST Risk Management Framework (RMF)		
National Institute of Standards and Technology – Special Publication 800-18	Guide for Developing Security Plans for Federal Information Systems		
National Institute of Standards and Technology – Special Publication 800-30	Guide for Conducting Risk Assessments		

Reference Document	Title	Mod	Effective Date (Contracting Officer Direction Date) and Relevant Notes
National Institute of Standards and Technology – Special Publication 800-34	Contingency Planning Guide for Federal Information Systems		
National Institute of Standards and Technology – Special Publication 800-37	Guide for Applying RMF to Federal Systems (current revision)		
National Institute of Standards and Technology – Special Publication 800-39	Managing Risk for Information Systems (current revision)		
National Institute of Standards and Technology – Special Publication 800-40 Rev. 4	Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology		
National Institute of Standards and Technology – Special Publication 800-46 Rev. 2	Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security		
National Institute of Standards and Technology – Special Publication 800-53	Security Controls for Federal Information Systems (current revision)		
National Institute of Standards and Technology – Special Publication 800-53A	Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans		
National Institute of Standards and Technology – Special Publication 800-59	Guideline for Identifying an Information System		
National Institute of Standards and Technology – Special Publication 800-60, Volume 1	Guide for Mapping Types of Information and Information Systems to Security Categories		
National Institute of Standards and Technology – Special Publication 800-60, Volume 2	Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices		
National Institute of Standards and Technology – Special Publication 800-61	Computer Security Incident Handling Guide		
National Institute of Standards and Technology – Special Publication 800-63-3	Digital Identity Guidelines		
National Institute of Standards and Technology – Special Publication 800-64	Security Considerations in the System Development Lifecycle		
National Institute of Standards and Technology – Special Publication 800-82	Guide to Industrial Control System (ICS) Security		
National Institute of Standards and Technology – Special Publication 800-88	Guidelines for Media Sanitization		
National Institute of Standards and Technology – Special Publication 800-122	Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)		
National Institute of Standards and Technology – Special Publication 800-125B	Secure, Virtual Network Configuration for Virtual Machine (VM) Protection		
National Institute of Standards and Technology – Special Publication 800-128	Guide for Security-Focused Configuration Management of Information Systems		

Reference Document	Title	Mod	Effective Date (Contracting Officer Direction Date) and Relevant Notes
National Institute of Standards and Technology – Special Publication 800-137	Information Security Continuous Monitoring for Federal Information Systems and Organizations		
National Institute of Standards and Technology – Special Publication 800-144	Guidelines on Security and Privacy in Public Cloud Computing		
National Institute of Standards and Technology – Special Publication 800-150	Guide to Cyber Threat Information Sharing		
National Institute of Standards and Technology – Special Publication 800-153	Guidelines for Securing Wireless Local Area		
National Institute of Standards and Technology – Special Publication 800-160, Volume 1	Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems		
National Institute of Standards and Technology – Special Publication 800-161 Rev 1	Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations		
National Institute of Standards and Technology – Special Publication 800-171	Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations		
National Institute of Standards and Technology – Special Publication 800-181	NIST National Initiative for Cybersecurity Education (NICE)		
National Institute of Standards and Technology – Special Publication 1800-10	Protecting Information and System Integrity in Industrial Control System Environments		
National Institute of Standards and Technology – Special Publication 1800-31	Improving Enterprise Patching for General IT Systems		
NIST Privacy Framework	A Tool for Improving Privacy through Enterprise Risk Management		
Department of Homeland Security	Handbook for Safeguarding Sensitive Personally Identifiable Information		
Department of Homeland Security -- Binding Operational Directive 23-01	Improving Asset Visibility and Vulnerability Detection on Federal Networks		
Department of Homeland Security -- Binding Operational Directive 23-01 Implementation Guidance	Implementation Guidance for CISA Operational Directive 23-01: Improving Asset Visibility and Vulnerability Detection on Federal Networks		
Department of Homeland Security -- Binding Operational Directive 22-01	Reducing the Risk of Known Exploited Vulnerabilities		
Department of Homeland Security -- Binding Operational Directive 20-01	Develop and Publish a Vulnerability Disclosure Policy		
Department of Homeland Security -- Binding Operational Directive 19-02	Vulnerability Remediation Requirements for Internet-Accessible Systems		
Department of Homeland Security -- Binding Operational Directive 18-02	Securing High Value Assets		
Department of Homeland Security -- Binding Operational Directive 18-01	Enhance Email and Web Security		
Department of Homeland Security -- Binding Operational Directive 17-01	Removal of Kaspersky-branded Products		
Department of Homeland Security -- Binding Operational Directive 16-03	2016 Agency Cybersecurity Reporting Requirements		
Department of Homeland Security -- Binding Operational Directive 16-02	Threat to Network Infrastructure Devices		

Reference Document	Title	Mod	Effective Date (Contracting Officer Direction Date) and Relevant Notes
Department of Homeland Security (DHS), Binding Operational Directive, BOD-15-01	Critical Vulnerability Mitigation Requirement for Federal Civilian Executive Branch Departments' and Agencies' Internet-Accessible Systems		
Department of Homeland Security – Emergency (Cybersecurity) Directives	All – implement as published		
Department of Homeland Security – Emergency Directive 19-01	Mitigate DNS Infrastructure Tampering		
Department of Homeland Security – Emergency Directive 20-02	Mitigate Windows Vulnerabilities from January 2020 Patch Tuesday		
Department of Homeland Security – Emergency Directive 20-03	Mitigate Windows DNS Server Vulnerability from July 202 Patch Tuesday		
Department of Homeland Security – Emergency Directive 20-04	Mitigate Netlogon Elevation of Privilege Vulnerability from August 202 Patch Tuesday		
Department of Homeland Security – Emergency Directive 21-01	Mitigate Solarwinds Orion Code Compromise		
Department of Homeland Security – Emergency Directive 21-02	Mitigate Microsoft Exchange On-Premises Product Vulnerabilities		
Department of Homeland Security – Emergency Directive 21-03	Mitigate Pulse Connect Secure Product Vulnerabilities		
Department of Homeland Security – Emergency Directive 21-04	Mitigate Windows Print Spooler Service Vulnerability		
Department of Homeland Security – Emergency Directive 22-03	Mitigate VMWare Vulnerabilities		
Homeland Security Presidential Directive (HSPD)-7	Critical Infrastructure Identification, Prioritization, and Protection		
Homeland Security Presidential Directive (HSPD)-12	Policies for a Common Identification Standard for Federal Employees and Contractors		
Department of Homeland Security, Federal Continuity Directive 1 (FCD 1)	Federal Executive Branch National Continuity Program and Requirements		
Department of Homeland Security, National Cybersecurity and Communications Integration Center (NCCIC)/United States Computer Emergency Readiness Team (US-CERT)	US-CERT Federal Incident Notification Guidelines		
U.S. General Services Administration	Federal Risk and Authorization Management Program (FedRAMP) Guidance – all – implement as published		
NNSA Supplemental Directive – NNSA SD 206.1	Privacy Program		
NNSA Supplemental Directive NNSA SD 206.2	Implementation of Personal Identity Verification for Uncleared Contractors		
NNSA Supplemental Directive – NNSA SD 226.1C	NNSA Site Governance		
NNSA Supplemental Directive – NNSA SD 251.1B	Directives Management		
NNSA Supplemental Directive – NA SD O 350.1	Management and Operating Contractor Service Credit Recognition		
NNSA Supplemental Directive – NNSA SD 415.1A	Project Oversight for Information Technology (PO-IT)		
NNSA Supplemental Directive – NNSA SD 430.1	Real Property Asset Management		

Reference Document	Title	Mod	Effective Date (Contracting Officer Direction Date) and Relevant Notes
NNSA Supplemental Directive – NNSA SD 452.2B	Nuclear Explosive Safety Evaluation Processes		
NNSA Supplemental Directive – NNSA SD 452.3	Managing the Operation of Shared NNSA Assets and Shared National Resources		
NNSA Supplemental Directive – NNSA SD 452.3-1A	Defense Programs Business Process System (DPBPS)		
NNSA Supplemental Directive – NNSA SD 452.3-2	Phase 6.X Process		
NNSA Supplemental Directive – NNSA SD 452.4-1	Nuclear Enterprise Assurance (NEA)		
NNSA Supplemental Directive – NNSA SD 470.4-2 Admin Chg 1	Enterprise Safeguards and Security Planning and Analysis Program		
NNSA Supplemental Directive – NNSA SD 471.6	Operations Security Program		
NNSA Supplemental Directive – NNSA SD 473.3	Enterprise Mission Essential Task List-based Protective Force Training Program		
ORR PCB FFCA	Oak Ridge Reservation Polychlorinated Biphenyl Federal Facilities Compliance Agreement		
PSLM	Primary Standards Lab Memorandum		
Technical Business Practices (TBP) and Infrastructure Business Practices (IBPs)	Technical Business Practices (TBP) and Infrastructure Business Practices (IBPs) For additional implementing information on TBPs visit the Defense Program Legacy (PRP Online) Home @ https://prp.sandia.gov/TBPs/Forms/AllItems.aspx For additional implementing information on IBPs visit the Defense Program Legacy (PRP Online) Home @ https://prp.sandia.gov/IBPs/Forms/AllItems.aspx		
RM 257945	AL-R8 Pit Matrix Requirements		

(A) Implementation of applicable directives.

(1) The Contractor shall submit an implementation plan to the Contracting Officer when required by the directive or other instruction of the Contracting Officer and within 60 days of the start of the Contract's Transition Period or within 60 days of the addition of a directive during contract performance.

(2) The Contracting Officer will approve or disapprove the plan and notify the Contractor of the decision. If the Contracting Officer disapproves the plan, he/she shall clearly identify all deficiencies and provide reasonable suggestions for making the plan acceptable. Within 30 days after notification of the disapproval of a plan, the Contractor shall submit to the Contracting Officer the revised plan for approval as described above.

(3) During the process of implementation, the Contractor will notify the Contracting Officer if modifications to the plan are required for any reason. The Contracting Officer will consider all such requests and will not unreasonably withhold his/her approval to modify such plans when circumstances warrant modification.

(B) Location of applicable directives and other noted items in above table

https://www.directives.doe.gov/
https://directives.nnsa.doe.gov/
https://directives.nnsa.doe.gov/delegations#b_start=0
https://www.nist.gov/
https://www.dhs.gov/department-homeland-security-management-directives
https://www.whitehouse.gov/omb/information-for-agencies/memoranda/
https://www.whitehouse.gov/omb/information-for-agencies/circulars/
https://www.federalregister.gov/presidential-documents/executive-orders
https://www.ecfr.gov/
https://uscode.house.gov/
https://www.archives.gov/about/laws
https://dl.dod.cyber.mil/wp-content/uploads/cyber-workforce/pdf/unclass-dod-manual-8140_03.pdf

End of Appendix