SUPPLEMENTAL DIRECTIVE

NNSA SD 205.1A

Approved: 09-24-24
Admin. Chg. 1: 04-03-25
Certification Due: 04-03-30

BASELINE CYBERSECURITY PROGRAM

NATIONAL NUCLEAR SECURITY ADMINISTRATION
Office of the Associate Administrator for Information Management and Chief Information Officer

CONTROLLED DOCUMENT
AVAILABLE ONLINE AT:
https://directives.nnsa.doe.gov/

OFFICE OF PRIMARY INTEREST (OPI):
Office of the Chief Information Officer

PRINTED COPIES ARE UNCONTROLLED

Change Summary

Directive Identification	Changes	Date	Version
SD 205.1A, *Baseline Cybersecurity Program*	1. Attachment 2, AT2-2, item m. Nuclear Weapon IT (NWIT). Removed 1st sentence "In accordance with SD 200.1, *Information Resources Management*, NWIT is…"	04-03-25	

THIS PAGE INTENTIONALLY LEFT BLANK

BASELINE CYBERSECURITY PROGRAM

1. PURPOSE. This Supplemental Directive (SD) defines the authorities, requirements, and responsibilities for the cybersecurity of information technology (IT), including national security systems (NSS), information systems, and operational technology (OT) within the National Nuclear Security Administration (NNSA). This SD supplements Department of Energy (DOE) Order (O) 205.1D, *Department of Energy Cybersecurity Program*, and incorporates the principles, processes, and oversight requirements in SD 226.1, *NNSA Site Governance,* current version, and is consistent with executive and Federal authorities.

2. AUTHORITY. Selected authorities are identified within this section. See Attachment 3, [References], for additional authorities.

   a. 44 United States Code (U.S.C.) 3551-3558 (2021).

   b. DOE O 205.1, *Department of Energy Cybersecurity Program*, current version.

3. CANCELLATION.

   SD 205.1, *Baseline Cybersecurity Program*, dated 7-7-2017.

4. APPLICABILITY.

   a. Federal. This SD applies to all NNSA Federal elements that acquire, operate, maintain, or dispose of information systems, including IT, NSS, and OT.

   b. Contractors. Except for the equivalencies and exemptions in paragraph 4.c., the Contractor Requirements Document (CRD), Attachment 1, and including Attachments 2 and 3, sets forth requirements that apply to management and operating (M&O) contracts.

   c. Equivalencies/Exemptions.

      (a) Equivalency. In accordance with the responsibilities and authorities assigned by Executive Order (E.O.) 12344, *Naval Nuclear Propulsion Program*, codified at 50 U.S.C. 2406 and 2511, and to ensure consistency throughout the joint Navy/DOE Naval Nuclear Propulsion Program, the Deputy Administrator for Naval Reactors (Director) will implement and oversee requirements and practices pertaining to this Directive for activities under the Director's cognizance.

      (b) Exemption. This SD does not apply to Sensitive Compartmented Information (SCI) IT located at NNSA sites. SCI systems must comply with Director of National Intelligence Directives and Orders and E.O. 12333, *United States Intelligence Activities*, accordingly, as advised by the DOE Director of Intelligence and Counterintelligence. Nothing in

this SD will alter or supersede the existing authorities of the Director of National Intelligence.

5. SUMMARY OF CHANGES.

a. Added requirements related to authority over nuclear weapons and nuclear weapon information technology (NWIT) and OT.

b. Revised requirements to include IT, including NSS and OT.

c. Updated requirements to align with NNSA Policy (NAP) 540.3, *Corporate Performance Evaluation Process for Management and Operating Contractors*.

d. Attachments removed for the creation of Technical Bulletins.

e. Incorporated Cybersecurity Supply Chain Risk Management (C-SCRM) considerations.

6. BACKGROUND.

This SD was developed using DOE O 205.1D, *Department of Energy Cybersecurity Program,* as a baseline and is tailored to meet the mission requirements of NNSA. It provides requirements to ensure the cybersecurity of information systems, including IT, NSS, and OT. This SD uses the term IT to generally represent the categories of IT, NSS, and information systems.

7. REQUIREMENTS. NNSA must develop and maintain a cybersecurity program (CSP) that:

a. Identifies, protects against, detects, responds to, and recovers from cybersecurity risks, issues, incidents, and associated trends.

b. Incorporates an enterprise architecture (EA) consistent with Zero Trust Principles.

c. Develops and manages the NNSA, both enterprise and site-specific CSP, along with enterprise and site-specific cybersecurity program plans (CSPP) that align with relevant DOE, NNSA, Committee on National Security Systems (CNSS), and Department of Defense (DoD) guidance. NNSA CSP and CSPP must incorporate the following concepts.

(1) Secure By Design. *Secure by design* means that technology products will be developed in a way that reasonably protects against malicious cyber actors successfully gaining access to devices, data, and connected infrastructure.

(2) Secure By Default. *Secure by default* means that the IT and OT default configuration should prioritize security. The cybersecurity controls should be enabled and enforced.

(3) Secure Operations. Cybersecurity controls and monitoring will continuously be improved to meet current and future cyber threats.

d. Ensures appropriate workforce training, experience, knowledge, and certifications commensurate with both job position description and responsibilities. All users of IT must complete annual cybersecurity training. NNSA Program Offices, Functional Offices, Field Offices, and M&O sites (NNSA Elements) must allow reciprocity of cybersecurity training requirements.

e. Incorporates governance boards that include NNSA Program Offices, Functional Offices, and Field Offices representatives as appropriate. The governance boards include the Enterprise Cybersecurity Advisory Board, Site Risk Management Councils, and Defense Programs Requirements Advisory Board.

f. Ensures IT and OT are authorized for use as a system or within a system boundary. System authorizations must align to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle approach for Security and Privacy*.

8. RESPONSIBILITIES.

a. Associate Administrator for Information Management and Chief Information Officer (NA-IM).

(1) Oversees cybersecurity requirements described in this directive for IT and OT, except for NWIT.

(2) Develops and implements an NNSA enterprise cybersecurity program and a cybersecurity program for NNSA Elements. Delegates this authority to qualified personnel, as needed.

(3) Serves as the Authorizing Official (AO) for NNSA IT and OT. Delegates this authority to qualified Federal NNSA Element personnel, as needed.

(4) Develops and publishes cybersecurity standards, processes, and procedures leveraging existing governance bodies in support of NNSA cybersecurity programs.

(5) Publishes system authorization documentation to enable reuse across DOE and NNSA to improve process efficiency. Delegates this authority to qualified personnel, as needed.

(6) Deploys and maintains enterprise cybersecurity infrastructure and technologies that meet current and future cyber threats.

(7) Develops and publishes strategies and proficiency standards, in coordination with the Associate Administrator for Management and Budget (NA-MB) and the Associate Administrator for Partnership and Acquisition Services (NA-PAS), to ensure NNSA Federal, support services contactor, and M&O contractor workforces possess the knowledge, skills, and abilities to meet their role-specific responsibilities. Role-specific responsibilities will align with and augment those described in NIST relevant Special Publications SPs.

(8) Designates an NNSA Chief Information Security Officer (CISO) to manage and oversee NNSA cybersecurity programs. The NNSA CISO duties include:

(a) Maintaining the CSSP, providing for cybersecurity services and requirements as appropriate.

(b) Conducting technical and programmatic cybersecurity assessments of NNSA IT and OT, except for NWIT, including those requirements as a delegated DoD CSSP. Performance of M&O contracts must be assessed against Performance Evaluation and Measurement Plans to provide formal feedback to the M&Os and input into the Fee Determinations in accordance with NNSA NAP 540.3, *Corporate Performance Evaluation Process for Management and Operating Contractors*.

(c) Develops, maintains, and publishes NNSA Information Condition (INFOCON) criteria. Executes changes to the NNSA INFOCON level as appropriate.

b. Deputy Administrator for Defense Programs (NA-10).

(1) Oversees the Nuclear Enterprise Assurance in direct accordance with SD 452.4-1, *Nuclear Enterprise Assurance)*.

(2) Maintains mission authority and mission risk acceptance for NWIT, including assurance throughout the nuclear weapon system lifecycle.

(3) Serves as the Authorizing Official for NWIT within NNSA and maintains applicable cybersecurity requirements for NWIT. Delegates this authority to qualified personnel, as needed.

c. Associate Administrator for Management and Budget (NA-MB).

(1) Develops and implements procedures necessary to recruit, retain, and develop cybersecurity personnel according to Office of Management and

Budget Memorandum M-16-15, *Federal Cybersecurity Workforce Strategy*, and the U.S Office of Personnel Management guide, *Compensation Flexibilities to Recruit and Retain Cybersecurity Professionals*.

(2) Develops and publishes strategies and proficiency standards, in coordination with NA-IM and NA-PAS, to ensure NNSA Federal, support services contactor, and M&O contractor workforces possess the knowledge, skills, and abilities to meet their role-specific responsibilities.

d. Associate Administrator for Partnership and Acquisition (NA-PAS).

(1) Develops and publishes strategies and proficiency standards, in coordination with NA-IM and NA-PAS, to ensure NNSA support services contactor and M&O contractor workforces possess the knowledge, skills, and abilities to meet their role-specific responsibilities.

e. NNSA Field Office Manager (FOM).

(1) Provides oversight for site-specific IT and OT, except for NWIT. Ensures all subject IT and OT systems have valid authorizations from the appropriately designated AO, following a defined Risk Management Framework (RMF) process that aligns to the Enterprise RMF program. This RMF process must leverage enterprise-offered cybersecurity standards, processes, tools, and services for site specific cybersecurity programs.

(2) Ensures, in coordination with system owners and M&O CISOs, that all subject IT and OT systems that are operated or maintained by the M&O are subject to routine audit, inspection, or assessment by the cognizant authorities. The periodicity of audits, inspections, and assessments may be established by the authorizing or auditing authorities.

(3) Nominates and coordinates with NA-IM to designate qualified personnel to act as authorizing officials from NNSA Field Offices. Authorizing officials may also be designated to approve enterprise-wide technologies managed by an M&O contractor.

f. NNSA Program/Functional Offices.

(1) Coordinate with NA-IM to designate qualified personnel to act as authorizing officials from NNSA Program and Functional Offices. Authorizing officials may also be designated to approve enterprise-wide technologies.

g. NNSA Contracting Officers.

(1) Include the CRD, Attachment 1, in any contracts that involve the acquisition of, or modification to IT products or services. Contracts must include applicable laws, regulations including, but not limited to, the Federal Acquisition Regulation and the DOE Acquisition Regulation, and DOE Directives required contract clauses.

(2) Issue annual IT and Cybersecurity Program Execution Guidance as part of the performance evaluation process for M&O contractors according to NNSA NAP 540.3, *Corporate Performance Evaluation Process for Management and Operating Contractors.*

(3) Assist originators of procurement requests who must incorporate this SD in new contracts, as appropriate.

9. REFERENCES. See Attachment 3.

10. DEFINITIONS. See Attachment 2.

11. CONTACT. The Office of the Associate Administrator for Information Management and Chief Information Officer at NNSAOCIO@nnsa.doe.gov.

BY ORDER OF THE ADMINISTRATOR:

Administrative Change approved: 04-03-2025

Attachments:
1. Contractor Requirements Document
2. Definitions
3. References

**ATTACHMENT 1: CONTRACTOR REQUIREMENTS DOCUMENT (CRD)
NNSA SD 205.1A, *BASELINE CYBERSECURITY PROGRAM***

1. INTRODUCTION.

This CRD establishes the requirements for National Nuclear Security Administration (NNSA) contractors who manage, operate, and have access to NNSA and Department of Energy (DOE) information systems, including information technology (IT), national security systems (NSS), and operational technology (OT). This CRD uses the term *IT* to generally represent the categories of IT, NSS, and information systems. Contractors must comply with the requirements listed in this CRD and all applicable attachments, which provide information to assist in the implementation of program requirements applicable to contracts in which this CRD is inserted.

Regardless of the performer of the work, the contractor is responsible for complying with the requirements of this CRD. The contractor is responsible for flowing down the requirements of this CRD to subcontractors at any tier to the extent necessary to ensure the contractor's compliance with the requirements. Government owned-contractor operated systems are subject to DOE CRD standards and requirements.

2. REQUIREMENTS. The CRD must be included in management and operating (M&O) contracts and the subcontracts to the M&O contracts that manage IT, including NSS, information systems, and OT. M&O contracts must include applicable Federal Acquisition Regulation and DOE Acquisition Regulations clauses.

Contractors must:

a. Develop and maintain a site-specific cybersecurity program plan that is consistent with the requirements provided by DOE and NNSA. The site-specific cybersecurity program plan must incorporate current and applicable Federal laws, regulations, policy, and guidance. Federal regulations, policy, and guidance include Office of Management and Budget (OMB) Circulars and Memoranda; Cybersecurity and Infrastructure Security Agency (CISA) and Director of the National Security Agency, Binding Operational Directives and Emergency Directives along with National Institute of Standards and Technology (NIST) best practices, NNSA cybersecurity standards, processes, and enterprise cybersecurity governing documents such as Incident Response Plans, Technical Bulletins, and Office of the Associate Administrator for Information Management and Chief Information Officer (NA-IM) Memoranda. The site-specific cybersecurity program plan must be approved by the Field Office Manager or designated representative.

b. Manage the site-specific cybersecurity program plan by integrating cybersecurity requirements in IT, OT, and nuclear weapon information technology (NWIT) to protect these systems in a secure manner commensurate with the risks, threats, vulnerabilities, and magnitude of harm relative to compromise.

c. Maintain, and obtain annual reauthorization of, a site-wide cybersecurity risk management strategy that aligns with the latest revision to NIST Special Publication (SP) 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle approach for Security and Privacy*.

d. Implement a risk managed approach to subcontractor requirements and monitoring program that is defined, documented and approved by the appropriately designated Authorizing Official (AO) and the NNSA Chief Information Security Officer (CISO), ensuring that implementation and ongoing monitoring of cybersecurity requirements related to IT, OT, and service contracts are implemented for all subcontractors. Exceptions must be reviewed by the AO and the NNSA CISO and approved by the contracting officer.

e. Implement a subcontractor quality assurance program that validates cybersecurity subcontract requirements commensurate with the risks, threats, and program costs.

f. Provide cybersecurity on all contractor IT and implement the security requirements in NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, in accordance with DOE Order 471.7, *Controlled Unclassified Information*, and Code of Federal Regulations 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*.

> If using a cloud service provider to store, process, or transmit any government information on a contractor IT in performance of their contract, the contractor must require and ensure that the cloud service provider meets security requirements equivalent to those established by the NNSA for Federal Risk and Authorization Management Program, for low, moderate, or high baseline systems based on the categorization of the system.

g. Acquire, operate, maintain, or dispose of IT and OT and government-related data according to contractual requirements unless reviewed by the AO and expressly authorized by the contracting officer.

h. Not access, use, or disclose government data unless specifically authorized.

i. Manage the attributes of their contractor assurance systems (CAS) in a risk-informed manner, ensuring key performance deliverables tied to compliance and mission sustainability while meeting the cybersecurity expectations as defined in SD 226.1, *NNSA Site Assurance and Oversight*.

(1) CAS must provide quarterly performance reporting in accordance with direction from the CISO.

(2) Performance results will be assessed against the Performance Evaluation and Measurement Plans and used to provide formal feedback.

(3) Subcontractor cybersecurity oversight measures must be included in the annual CAS and the contractor performance evaluation process.

j. Ensure all contractors and subcontractors have policies and processes to address supply chain management, System Development Life Cycle and Software Bill of Materials as noted in NIST SP 800-161, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*.

k. Comply with and provide support to assessments and inspections conducted by the Office of the Associate Administrator for Information Management and Chief Information Officer (NA-IM) assessment team and the Mission Owner, to include participating and responding to external inspections and audits conducted by the Office of the Inspector General, the Government Accountability Office, and the Office of Enterprise Assessments.

l. Require annual self-assessments of the site-specific cybersecurity plan. For NWIT, require assessments in accordance with the NWIT risk management framework.

m. Fulfill annual Contractor Performance Evaluation Plan, Project Execution Plan, Performance Evaluation Report, and Performance Execution Guidance requirements. Artifacts showing the site has met the deliverables must be reviewed by the Authorizing Official and reported to NA-IM.

n. Implement or leverage enterprise cybersecurity standards, processes, enterprise cybersecurity infrastructure and technologies, and system authorization and accreditation documentation in the enterprise cybersecurity Governance, Risk, and Compliance (GRC) system. Sites that implement site-specific GRC systems must ensure this documentation is communicated across a system interface with the enterprise GRC system.

o. Ensure all contractors and subcontractors with cybersecurity responsibilities for overseeing and managing Federal information and information systems and networks are appropriately trained and capable of performing their specified roles.

p. Implement a Zero Trust Architecture framework in accordance with CISA and OMB guidelines.

q. Report cybersecurity incidents in accordance with the Enterprise Incident Response Plan. Notify the Mission Owner if a suspected incident impacts the nuclear weapons program.

3. RESPONSIBILITIES.

a. Contractor's Senior Officer (Director, President, Laboratory Manager, or designee).

(1) Ensures their site develops and maintains a comprehensive cybersecurity program that employs a Risk Management Framework (RMF) based on the acceptable risk levels set by the site Field Office Manager (FOM), or delegate, and Mission Owners, and is identified in the Site Risk Management Plan.

(2) Ensures their site develops a CAS based on the attributes outlined in SD 226.1, *NNSA Site Assurance and Oversight*, and the requirements of this policy.

(3) Ensures appointment of a contractor representative to participate on the Enterprise Cybersecurity Advisory Board (ECSAB) in conjunction with the FOM and the AO, who serves as a default member.

(4) In coordination with the M&O CIO, FOM, and AO, ensures establishment of the Site Risk Management Council (SRMC) and appointment of council members.

(5) Ensures governance for the safe, secure, and trustworthy development and use of artificial intelligence (AI).

b. M&O Chief Information Officer (CIO).

(1) Working with the Contractor's Senior Officer, assists in executing an effective Cybersecurity Program (CSP) in accordance with federal laws and the requirements and responsibilities within this CRD and all applicable attachments.

(2) Assumes the operation of systems in accordance with the site's approved risk management plan. Makes risk management recommendations to the Senior Contractor Official and manages the implementation of the site CSP.

(3) Validates the qualifications of an individual appointed as an Information System Security Manager, in collaboration with the AO, who will be responsible for direct oversight of development and implementation of the CSP at the M&O site.

(4) Ensures establishment of SRMC and appointment of council members in conjunction with the Contractor's Senior Officer, FOM, and AO.

(5) Participates in governance for the safe, secure, and trustworthy development and use of AI.

c. Contractor/Site System Owner.

(1) Acquire, operate, maintain, and dispose of IT and OT systems according to Federal regulations throughout the system lifecycle.

(2) Address the operational interests of the user community (i.e., users who require access to systems to satisfy mission, business, or operational requirements) and ensure compliance with security requirements.

(3) Develop and maintain the security plan and ensure the system is deployed and operated in accordance with the agreed-upon security controls, in coordination with the AO.

(4) Decide who has access to the system (and what types of privileges or access rights) and ensure that system users and support personnel receive the requisite security training, in coordination with the information owner.

(5) Inform organizational officials of the need to conduct security authorizations and assessments; ensure the necessary resources are available for the effort; and provide the required system access and documentation to the security control assessor, with authority from the AO.

(6) Receive the security assessment results from the security control assessor, take action to reduce or eliminate vulnerabilities, assemble the authorization package, and submit it to the AO, or AO designated representative, for adjudication.

(7) Participate in the SRMC and ECSAB, as needed.

(8) Coordinate all RMF activities with the AO to ensure the risk posture, documentation, risk mitigation, and continuous monitoring of the IT or OT system and ensure the appropriate alignment of the NNSA authorization boundary.

d. Site Risk Management Council.

(1) Develop a charter that defines processes and the site's membership and activities, and issue work plans that align with the requirements of this SD and both the Enterprise Cybersecurity Program Plan and site-specific CSPP, in collaboration with contractor management.

(2) Submits unmitigated cybersecurity risks and issues to the ECSAB.

(3) Notifies AOs regarding communications with the ECSAB and guidance or direction from the CIO.

THIS PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT 2: DEFINITIONS

This Attachment applies to National Nuclear Security Administration (NNSA) Federal and contractor organizations.

a. Authorizing Official (AO). A senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations and assets, individuals, other organizations, and the Nation. The Enterprise AO is appointed by the Chief Information Officer (CIO). The AO should have the authority to oversee the budget and business operations of the system within the Sites. Additionally, the AO develops cybersecurity requirements, plans and operational information system security policies for each system, program, and site for which the AO has approval authority, and maintains documentation for enterprise information system authorizations. The AO has inherent U.S. Government authority and, as such, must be a Federal employee.

b. AO Designated Representative. Acts on behalf of the AO in coordinating and carrying out the necessary activities required during the Security Authorization of an information system. The only activity that cannot be delegated by the AO is the Security Authorization decision and the signing of the associated authorization decision document. Not required to be a Federal employee but must be appointed by the AO and report to the AO.

c. Cybersecurity and Infrastructure Security Agency. A component of the U.S. Department of Homeland Security responsible for cybersecurity and infrastructure protection across all levels of government.

d. Chief Information Security Officer (CISO). Senior Agency Information Security Officer with information system or security management/oversight responsibilities. Serves as the principal security leader for NNSA to implement requirements of Federal Information Security Modernization Act and as the CIO liaison and implementation manager to Federal agencies for all matters relating to security and the NNSA Cybersecurity Program.

e. Cybersecurity Program Plan (CSPP). A management-level document detailing the organization's procedures and practices for ensuring effective cybersecurity.

f. Cybersecurity Incident. An occurrence that actually or imminently jeopardizes the integrity, confidentiality, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

g. Enterprise Cybersecurity Advisory Board (ECSAB). The ECSAB advises the NNSA CIO and the NNSA Enterprise on cybersecurity and IT budget risk and provides a common approach to determine and manage residual risk within identified thresholds and determines risks affecting the enterprise.

h. Information Owner. Federal or contractor official(s) holding statutory, management, or operational authority for information residing on information systems and the responsibility for establishing the policies and procedures governing its generation, collection, processing, dissemination, and disposal.

i. Information System. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

j. Information System Security Manager (ISSM). An individual appointed by the CISO to manage Federal information systems with critical knowledge of systems functionality, enterprise cybersecurity policies, and security measures to prevent unnecessary vulnerabilities to enterprise information or information systems.

k. Information Technology. With respect to an executive agency means (A) any equipment of an interconnected system, or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use (i) of that equipment; or (ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product; (B) includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware, and similar procedures, services (including support services), and related resources; but (C) does not include any equipment acquired by a Federal contractor incidental to a federal contract, 40 U.S.C. 11101(6).

l. Mission Owner. The senior official or executive within an organization with specific mission or line of business responsibilities and has a security or privacy interest in the organizational systems supporting those missions or lines of business. Provides inputs to the risk management strategy, plays an active part in the system lifecycle, and serves in the role of authorizing official, as applicable.

m. Nuclear Weapon IT (NWIT). An information system or components of an information system integral to a nuclear weapon; surrogates for nuclear weapons used in development, test, or training; and equipment connecting to nuclear weapons or their surrogates, including war reserve units, developmental units, weapon components, test units, trainer units, and weapon operational support equipment (e.g., systems that are directly involved in operational test, configuration, security, and safety throughout the lifecycle).

n. Officially Designated Federal Security Authority (ODFSA). Along with the appropriate program authority and Contracting Officer Representative, the ODFSA is the individual who accepts unmitigated residual risk, in writing, for TEMPEST, Protected Distribution Systems, and Wireless Network Security, in accordance with Intelligence Community

Directive 702, *Technical Surveillance Countermeasures*, DOE O 470.6, *Technical Security Program,* and SD 470.6, *Technical Security Program*.

o. Operational Technology (OT). Hardware and software that detects or causes a change through the direct monitoring or control of physical devices, processes, and events in the enterprise, 15 U.S.C. Section 278g-3a (6).

p. Site Risk Management Council. Responsible for managing information management risks at their respective sites, serving as a common resource for stakeholders. Also supports Federally appointed AOs in managing risks associated with information systems within their responsibility.

q. System Owner. An official with statutory or operational authority for specified information and responsibility for establishing the controls governing its generation, collection, processing, dissemination, and disposal. The owner or steward of the information processed, stored, or transmitted by an information system may or may not be the same as the system owner. A single information system or OT system may contain information from multiple information owners.

THIS PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT 3: REFERENCES

This Attachment applies to National Nuclear Security Administration (NNSA) federal and contractor organizations.

1. 6 United States Code (U.S.C.) 681b et seq., as amended by the *Cyber Incident Reporting for Critical Infrastructure Act of 2022*, Public Law (Pub. L.) 117-103.

2. 15 U.S.C. 278g-3a, *Definitions*.

3. 40 U.S.C. 11103, *Applicability to national security systems*.

4. 44 U.S.C. 3541 et seq., as amended by the *Federal Information Security Modernization Act of 2014*, Pub. L. 113-283, and the *Federal Information Security Management Act of 2002*, Pub. L. 107-347.

5. 32 Code of Federal Regulations (CFR) Part 2002, *Controlled Unclassified Information (CUI)*.

6. 48 CFR 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*.

7. Executive Order 14028, *Improving the Nation's Cybersecurity*, dated 5-12-2021.

8. Office of Management and Budget (OMB) Memorandum M-16-15, *Federal Cybersecurity Workforce Strategy*.

9. NIST Special Publication (SP) 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, current version.

10. NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, current version.

11. NIST 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, current version.

12. U.S. Office of Personnel Management guide, *Compensation Flexibilities to Recruit and Retain Cybersecurity Professionals*.

13. Intelligence Community Directive 702, *Technical Surveillance Countermeasures.*

14. Department of Energy (DOE) Order (O) 205.1, *Department of Energy Cybersecurity Program*, current version.

15. DOE O 226.1, *Implementation of Department of Energy Oversight Policy*, current version.

16. DOE O 471.7, *Controlled Unclassified Information*, current version.

17. DOE O 470.6, *Technical Security Program*, current version.

18. Supplemental Directive (SD) 226.1, *NNSA Site Assurance and Oversight*, current version.

19. SD 452.4-1, *Nuclear Enterprise Assurance (NEA)*, current version.

20. SD 470.6, *Technical Security Program*, current version

21. NNSA Policy (NAP) 540.3, *Corporate Performance Evaluation Process for Management and Operating Contractors*, current version.