U.S. Department of Energy
Washington, DC

ORDER

DOE O 205.1D

Approved: 4-30-2024

SUBJECT: DEPARTMENT OF ENERGY CYBERSECURITY PROGRAM

1. PURPOSE. This Order enables the Department of Energy (DOE) to accomplish its mission and fulfill Federal cybersecurity requirements. Additionally, this Order allows Departmental Elements (DEs) programmatic and operational flexibility to tailor their cybersecurity posture by utilizing risk management, enabling effective implementation, and delegating risk management to the lowest appropriate level. Finally, this Order addresses roles and responsibilities, and sets standards for performance across all Department levels.

2. CANCELS/SUPERSEDES. DOE O 205.1C Chg 1, *Department of Energy Cyber Security Program*, dated February 3, 2022. Cancellation of a directive does not, by itself, modify or otherwise affect any contractual or regulatory obligation to comply with the directive. Contractor Requirements Documents (CRDs) that have been incorporated into a contract remain in effect throughout the term of the contract unless and until the contract or regulatory commitment is modified to either eliminate requirements that are no longer applicable or substitute a new set of requirements.

3. APPLICABILITY.

   a. Departmental Applicability. Except for the equivalencies/exemptions in paragraph 3.c., this directive applies to all DEs that develop, operate, or manage DOE information systems and/or devices, and any personnel who use DOE information systems and/or devices.

      (1) The Administrator of the National Nuclear Security Administration (NNSA) must assure that NNSA employees comply with their responsibilities under this directive. Nothing in this directive will be construed to interfere with the NNSA Administrator's authority under section 3212(d) of Public Law (P.L.) 106-65 to establish Administration-specific policies, unless disapproved by the Secretary (S1).

      (2) The Administrator of the Bonneville Power Administration (BPA) must ensure that BPA employees and contractors comply with the responsibilities and objectives of this directive where applicable in accordance with the Bonneville Administrator's authorities under Public Law (P.L.) 75-329 (16 U.S.C. Ch. 12B, Bonneville Project Act of 1937), P.L. 93-454 (16 I.S.C. Chapter 12G, Federal Columbia River Transmission System Act of 1974), and P.L. 96-501 (Pacific Northwest

Electric Power Planning and Conservation Act; 16 U.S.C. Chapter 12H), among other statutes specific to BPA. DOE Contractors. Except for the equivalencies/exemptions in paragraph 3.c., the CRD, Attachment 1, sets forth requirements of this Order that will apply to all Management and Operating (M&O) contracts; non-M&O major site/facility contracts; and other non-M&O contracts as determined by the HDE that collect, create, process, transmit, store, or disseminate data on information systems and operational technology (OT) for DOE or on the behalf of DOE. The CRD also forms the basis for equivalent requirements, that must be included in contract clauses or other contract provisions, applicable to non-M&O contracts that collect, create, process, transmit, store, or disseminate data on information systems.

(3) DOE contractors must comply with applicable laws and requirements identified in the CRD.

b. Equivalencies/Exemptions for DOE O 205.1D.

(1) Equivalency. In accordance with the responsibilities and authorities assigned by Executive Order 12344, codified at Title 50 United States Code (U.S.C.) sections 2406 and 2511 and to ensure consistency through 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, as deemed appropriate.

(2) Exemptions. None.

4. REQUIREMENTS. The DOE Cybersecurity Program is a shared, distributed enterprise risk management approach to protect DOE information systems. It complies with the Federal Information Security Modernization Act of 2014 (FISMA 2014) and aligns with Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*, the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) of NIST Special Publication (SP) 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, and the NIST Framework for Improving Critical Infrastructure Cybersecurity – abbreviated as Cybersecurity Framework (CSF).

The DOE Cybersecurity Program is defined by the core cybersecurity functions that are based on the NIST CSF. Collectively, these functions enable DOE to provide mission and operational resilience under any cybersecurity situation or condition and allow us to act collectively, consistently, and effectively in our own defense.

The DOE Cybersecurity Program approaches implementation of cybersecurity requirements in a manner commensurate with impact to mission, national security, risk, and magnitude of harm. Risks include the results from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained

by or on behalf of the DOE, or the information systems used or operated by DOE or by a DOE contractor or other organization on behalf of DOE. It also confirms authorities and assigns responsibilities for protecting information and information systems that store, process, or transmit DOE electronic information from cyber intrusions and addresses both information technology (IT) and OT systems, as well as the Internet of Things (IoT).

The DOE Cybersecurity Program empowers Heads of Departmental Elements (HDEs) and provides them with the flexibility to tailor and implement cybersecurity risk mitigation controls in consideration of threats and harms, acceptable risks, mission needs, and environmental and operational factors. Risk management will be performed in accordance with other DOE Directives, as applicable.

In addition to complying with the Department's Cybersecurity Program Requirements stated herein, DEs must observe requirements stated as law, obligation, and/or government-wide policy stemming from governance bodies external to the department, such as other Federal Agencies, Congress, or the White House, in particular for categories of information systems requiring specialized controls or reporting as listed below. Where required by law, policy, or Departmental Directive, DEs must document and implement compliance approaches stemming from these requirements in the applicable Cybersecurity Program Plan (CSPP). For Power Marketing Administration (PMA) information systems that meet the criteria for North American Electric Reliability Corporation (NERC) governance, DEs/Sites must comply with the Critical Infrastructure Protection standards.

Additionally, the DOE Cybersecurity Program sets the framework to protect its National Security Systems (NSS) with the requirements of the Committee for National Security Systems (CNSS). DOE classified systems are designated as NSS. Requirements for NSS are specifically identified within this Order.

a. **NIST CSF Function: Govern**

(1) To implement the DOE Cybersecurity Program, the following must be developed and maintained:

(a) Enterprise Cybersecurity Program Plan (E-CSPP), which is the responsibility of the DOE Chief Information Security Officer (CISO) to manage, in consultation with the DOE Chief Information Officer (CIO) and in coordination with HDEs. The E-CSPP must address the NIST RMF steps and the CSF from the Department’s overall organizational perspective.

1 An E-CSPP must be implemented and executed by DOE Chief Information Security Officer (CISO) and address this Order, in accordance with the Federal laws, regulations, directives, policies, standards, and guides pertaining to cybersecurity.

2 The E-CSPP must be reviewed and updated annually or if a major change occurs within the environment.

3 The E-CSPP must address the exception and exemption processes for information security controls.

(b) Departmental Element Cybersecurity Program Plans (DE-CSPPs), which must cover all DE systems and IT and OT assets. Consolidated, combined, or subordinate CSPPs may be used as needed to address organizational structures, shared service arrangements, and mission requirements. DE-CSPPs must address the CSF alignment and the RMF steps from their organizational, mission/business, and system perspectives.

1 Each DE must be covered by a CSPP or implement a CSPP by adopting another DE's CSPP based on organizational structure, shared services, or mission needs. DE-CSPPs must address this Order.

2 The DE-CSPP needs to be reviewed annually and updated based on E-CSPP updates.

3 The DE-CSPP must also address:

a Zero Trust Architecture (ZTA) Implementation

i. Each DE must develop a ZTA Implementation Plan based on the Office of the Chief Information Officer's (OCIO's) *Improving Cybersecurity: Guide to Implement Zero Trust Architecture*. The Plan must be updated annually.

b Cloud Security.

i. Each DE must address security requirements for cloud computing and use of Federal Risk and Authorization Management Program (FedRAMP) processes and tools, as applicable in accordance with Federal laws, regulations, directives, policies, standards, and guides pertaining to cybersecurity, as well as interrelated DOE issuances, directives, policies, and procedures.

c Security Operations Center (SOC) Implementation and Maintenance.

i. Each DE with a SOC must develop a SOC Plan that documents their SOC implementation and maintenance efforts. The plan must be updated annually.

d The DE-CSPP must address the exception and exemption processes for information security controls.

(2) Measures of Performance.

(a) Establish cybersecurity performance metrics in addition to the baseline metrics defined by OCIO that measure mission outcomes.

(b) Implement processes for collecting and reporting cybersecurity data and metrics required by Federal law, regulation, or policy.

(c) Define processes with applicable Contracting Officers (COs) to evaluate contractor programs, management, and assurance systems, for effectiveness of performance, consistent with DOE O 226.1, *Implementation of Department of Energy Oversight Policy*, and related contract terms and conditions.

(d) Establish processes for Plan of Action and Milestones (POA&M) tracking and reporting cybersecurity weaknesses identified for information systems that integrate with continuous monitoring and risk management processes.

(3) Exception and Exemption Process for Information Security Controls. The Process must be documented in the site's CSPP and allow:

(a) A waiver to be obtained from the Authorizing Official (AO) for any exceptions to allow access to specific resources and/or sites or exemptions from requirements in its entirety;

(b) DEs to inherit controls from OCIO as applicable; and

(c) DEs to manage a repository for any exceptions and exemptions.

(4) Warning Banner. DOE, NNSA, NSS, and Federal unclassified systems must display a system use notification (e.g., Warning Banner) at login and require users to electronically acknowledge the warning (such as clicking on "OK" or "I agree" button to proceed). The Warning Banner must cover the following in substance:

(a) That by using the account or the information system, or connecting any devices to the information system, the user acknowledges, understands, and consents to certain identified actions;

(b) The user acknowledges, understands, and consents to the fact that the user has no reasonable expectation of privacy regarding communications or data transiting or stored on the information system or devices connected to the information system;

(c) The user acknowledges, understands, and consents to the fact that at any time and for any official purpose, the government may monitor, intercept, record, and search any communications or data transiting or stored on the information system or devices connected to the information system;

(d) The user acknowledges, understands and consents to the fact that any communications or data transiting or stored on the information system or devices connected to the information system may be used or disclosed for any official purpose, including to law enforcement or other government agencies, as deemed appropriate by DOE, or as mandated by law.

(e) In addition to the minimum requirements set forth above it is recommended that usage banners, policies, and user agreements collectively will provide, in some form, for the following:

1 The user acknowledges, understands, and agrees to be bound by requirements for use of government information systems;

2 The user acknowledges, understands, and consents to the fact that unauthorized or improper use of Government information systems may result in limitations placed on the use of Government information systems, disciplinary or adverse actions, including termination of employment, criminal penalties, and or financial liability for the cost of such improper use;

3 The user will appropriately access, manage, and safeguard any federal records and information stored within this system, including controlled unclassified information (CUI).

4 To the extent the user has any questions concerning use of government information systems, the user will consult with their supervisor or other appropriate person; and

5 To the extent the usage banners satisfy the above provisions, such banners will be deemed to comply with DOE O 470.5, *Insider Threat Program*

b. **NIST CSF Function: Identify**

(1) Asset Management.

(a) Endpoints.

1 Ongoing, reliable, and accurate asset inventories must be created and maintained to include both IT and OT hardware and software. Endpoints must abide by the requirements in Binding Operational Directive (BOD) 23-01, *Improving Asset Visibility and Vulnerability Detection on Federal Networks*.

(b) Software.

1 All software subject to the requirements of OMB Memorandum (M) 22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*, and OMB M 21-30, *Protecting Critical Software Through Enhanced Security Measures*, must be identified and inventoried.

(c) High Value Assets (HVA).

1 HVAs must comply with requirements detailed in OMB M 19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*. This includes developing, maintaining, and regularly updating HVA inventory lists, at a minimum, on an annual basis.

(d) DOE Cybersecurity Data Repository.

1 A DOE Cybersecurity Data Repository must be established and maintained for key cybersecurity information. The Data Repository facilitates enterprise visibility and bi-directional information flows on key items for effective cybersecurity operations. The repository must be updated with input from personnel outside of the program element, and include the following items:

a Inventories.

i. FISMA Systems and status. Name of FISMA System, applicable identification for enhanced controls, and AO contact information.

ii. Internet-facing Internet Protocol addresses and websites.

iii. Financial systems.

iv. Unclassified and Classified NSS.

b Cybersecurity Posture.

i. DE/Site POA&Ms for:

- HVAs - Updates for any open items.
- Issues that cannot be closed in less than 30 days or require significant resources to close.
- Issues for Oversight Audits and Assessments including DOE Enterprise Assessments (EA), Government Accountability Office (GAO) and Office of Inspector General (OIG).

ii. DE/Site Cybersecurity Risk Register.

iii. DE/Site current and target NIST CSF Profiles.

c Names and Contact Information.

i. DE/Site individuals for cybersecurity incident response, coordination and notification covering normal business hours and non-business hours.

ii. DE/Site CIO, CISO, Information Systems Security Managers/Information Security Site Managers, System Owners (SO), or individuals performing similar functions.

iii. DE/Site AO.

iv. DE/Site designated representatives for routine cybersecurity data collection and reporting.

d Identification of systems that are HVAs.

e Identification of systems that contain CUI.

(2) Business Environment.

(a) Establish and maintain a Cyber Supply Chain Risk Management (C-SCRM) program that is a cooperative effort among

procurement, cybersecurity, legal, IT operations, system stakeholders, and risk management officials.

(b) Per Presidential Policy Directive (PPD)-21, *Critical Infrastructure Security and Resilience*, DOE is to collaborate with the Nuclear Regulatory Commission (NRC), as appropriate, on strengthening critical infrastructure security and resilience.

(3) Risk Assessment.

(a) DEs must update the:

1 Cybersecurity Risk Register on a quarterly basis; and

2 Current and Target NIST CSF Profiles on an annual basis.

(b) Every DOE system must have POA&Ms developed, implemented, and tracked for status reporting if an issue is found.

(c) Threat Awareness Program.

1 The OCIO must create procedures to share common threats, vulnerabilities, and incident-related information with the appropriate organizations.

2 The OCIO must identify sources of cyber threat information and a process for sharing the information, as appropriate.

3 Threats, vulnerabilities, likelihoods, and impacts must be appropriately identified and considered to assess cybersecurity and/or supply chain risks.

4 Both internal and external threats must be identified and documented.

5 Joint management of the DOE enterprise cybersecurity threat assessment with the Office of Intelligence and Counterintelligence (IN) and in coordination with DEs. Technical Threat assessments must include input from the Office of Environment, Health, Safety and Security (EHSS) and the NNSA per the CNSS and other policies for threats to information systems from technical means such as technical surveillance countermeasures (TSCM) and TEMPEST.

(4) Risk Management Strategy.

(a) A framework for establishing acceptable risk in the context of mission performance and assurance must be developed in accordance with OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, and other applicable guidance.

(b) Incorporate a methodology and model for contractors for graded oversight that is based on risk and the contractor's past performance in risk management and tailored to meet mission needs.

(c) Must provide flexibility to tailor cybersecurity protections based on risk assessments to cost-effectively reduce information security risks to an acceptable level.

(d) Must utilize a partnership approach that includes the AO and consultations with the Mission and SO in establishing acceptable risks.

(e) Enterprise Cybersecurity Risk Management.

1 Enterprise Risk Management policies and processes implemented must:

a Manage the level of risk.

b Provide support for making informed enterprise-level cybersecurity risk decisions.

c Manage organization-wide cybersecurity risk assessment that include aggregation of system-level risk assessments.

(f) The DOE OCIO will establish, maintain, and document the standards for delegation of AOs across the organization and will reserve the right to rescind AO delegations in violation of documented standards.

1 DOE OCIO will maintain a repository of documented standards as they relate to AO delegation.

(g) Assessment and Authorization (A&A) Process.

1 The A&A process verifies that DOE systems, including cloud and externally-hosted systems, are FISMA-compliant.

2 Must address management of common controls for any systems that fall under the sites' purview.

3 Must have processes for establishing, maintaining, and terminating written agreements as applicable for interconnection of system(s), revision when significant changes occur, and review on a defined risk-based periodicity.

4 Appropriate Program Authority (APO/Continued Service Agreement (CSA)/Officially Designated Federal Security Authority (ODFSA)/Contracting Officer Representative (COR)) must accept unmitigated residual risk, in writing, in accordance with Intelligence Community Directive (ICD) 702, Technical Security and Signals Countermeasures (TSSC), and DOE O 470.6, *Technical Security Program* (TSCM, TEMPEST, Protected Distribution System (PDS), and Wireless Network Security (WiSEC)).

5 Existing systems retain authorization to operate until reauthorization is required (e.g., the systems have passed the authorization expiration date or because of significant security changes in the security requirements of the information system). For contractors to fully assess the CRD the DE-CSPPs must be in place before requesting an assessment of effects.

6 Authorizations can be granted either with, or without, restrictions or limitations.

a Authorizations with conditions (e.g., conditional Authorizations to Operate (ATOs)) should allow for sufficient time to allow the conditions to be satisfied.

b Once the conditions are satisfied, a new unrestricted ATO will be granted for the remainder of the specific A&A process' ATO length.

7 Extension of a current ATO system will not exceed one year (365 days) and may only be requested under one of the conditions listed below. The system must continue to maintain its A&A documentation (e.g., System Security Plan, Contingency Plan, POA&Ms). All actions to satisfy the conditions below must be completed within the extension period (e.g., no longer than 12 months).

a Transitioning to ongoing authorization;

b Planning for disposal;

c Consolidating into another system with an ATO. The scope of consolidation shall be approved by the AO and in consultation with the DE/Site CISO prior to submitting the ATO extension request;

d Transitioning into a cloud environment with an ATO. The scope of the transition into the cloud environment shall be approved by the AO and in consultation with the DE/Site CISO prior to submitting the ATO extension request;

e Re-competing the system's contract;

f Completing the upgrade/replacement of major infrastructure components; or

g Completing the system's security assessment has been delayed due to contract issues.

8 Systems containing personally identifiable information (PII) must also follow requirements as specified in DOE O 206.1, *Department of Energy Privacy Program*.

9 Abide by the Federal Risk and Authorization Management Program (FedRAMP) Authorization Act per H.R. 7776, National Defense Authorization Act for Fiscal Year 2023, and subsequent OMB guidance applicable to the Act, and the DOE FedRAMP Agency Authorization Process.

10 No procurement for cloud products/services shall be completed without having obtained a valid ATO/authorization to use (ATU) granted by an AO in accordance with review of the FedRAMP provisional authorization.

11 Records contained in an information system must be managed in electronic format in accordance with an authorized federal records schedule and DOE O 243.1, *Records Management Program*.

(5) Cyber Supply Chain Risk Management (C-SCRM).

(a) For third-party suppliers, audits requirements must include a review of the provider's system and organization controls 2 Type 2 report, validating their assertion of maintaining minimum security controls to protect the information systems and data. If such

reports are restricted due to the sensitivity of their nature, at a minimum, a review of the vendor's system and organization controls 3 report should be done before initiating the vendor's services.

(b) For third-party suppliers, must ensure a provision is included in the contract agreement that protects from a Vendor-lock-in, preventing leaving, migrating, or transferring to an alternate provider, in the case of a dispute or due to a technical or non-technical constraint.

(c) All Federal Information Processing Standard (FIPS) 199 High, Moderate, and Low Impact systems must manage risks to their supply chain in accordance with NIST SP 800-161, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, including assessing supply chain risk from suppliers and third-party partners.

(d) Must require appropriate personnel to assess a supplier’s and third-party partner’s supply chain before acquisition as part of contract requirements and as necessary thereafter. Assessments may consist of audits, tests, or other forms of evaluation as deemed necessary.

(e) For Critical Software, must abide by the critical software requirements per OMB M 21-30.

(f) For Software Supply Chain Security, must abide by the software supply chain security requirements per Executive Order (EO) 14028, OMB M 22-18, and OMB M 23-16.

c. **NIST CSF Function: Protect**

(1) Identity Management and Access Control

(a) The enterprise architecture must move towards ZTA and an end state where every distinct application is run inside of its own perimeter (or is itself its own perimeter) and is treated as internet accessible.

1 Enforce and manage zero trust principles for both the cloud and on-premises environments.

(b) Centralized identity management systems must be employed for users that can be integrated into applications and common platforms.

(c) Strong phishing-resistant Multi-Factor Authentication (MFA) must be used throughout the Department.

1 Phishing-resistant MFA must be enforced on all networks, applications, endpoints, and systems.

2 For DOE staff, contractors, and partners, phishing-resistant MFA is required to access DOE-hosted accounts. DOE systems must discontinue support for authentication methods that fail to resist phishing, including protocols that register phone numbers for Short Message Service (SMS) or voice calls, supply one-time codes, or receive push notifications.

3 Phishing-resistant MFA shall be used when implementing any cloud service, application, or tool, and when accessing any cloud system via a network.

4 When authentication is required for public users, phishing-resistant MFA must be an option available on public-facing systems.

5 Password policies must not require use of special characters or regular rotation once phishing-resistant MFA is implemented and mandatory for that system.

6 When authorizing users to access resources, refer to OMB M 22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*.

7 Mobile devices access to systems must be authorized and managed to ensure they are approved and are securely configured. See Attachment 4 Portable Electronic Device Security.

8 For foreign national access to systems, refer to DOE O 142.3, *Unclassified Foreign National Access Program*.

9 Must require all network users to log onto the network with a two-factor Personal Identity Verification (PIV) card or other phishing-resistant credential meeting the NIST requirements for Identity Assurance Level 3 (IAL3) and Authenticator Assurance Level 3 (AAL3).

10 Federal system endpoints must be covered by an intrusion prevention system (IPS), anti-exploitation capabilities, and an antivirus (AV) solution that provides file reputation services that check suspicious files against continuously updated malware information in near real-time.

(d) Network Environment

1 Must resolve Domain Name System (DNS) queries using encrypted DNS wherever it is technically supported. Additionally, all DOE sites operating DNS resolvers must use DNS protection capabilities provided by the Cybersecurity and Infrastructure Security Agency (CISA).

2 Must enforce Hypertext Transfer Protocol Secure (HTTPS) for all web and application program interface (API) traffic in their environment. Must work with CISA to preload .gov domains into web browsers as only accessible over HTTPS.

3 All websites and/or internet-facing services connecting to the cloud-based service must meet the criteria for establishing secure connections as stated in the OMB M 15-13, *Policy to Require Secure Connections across Federal Websites and Web Services*, which specifies all connectivity must be HTTPS-only and implement HTTP Strict Transport Security (HSTS).

(e) Application Workload

1 Must operate dedicated application security testing programs.

2 Must utilize high-quality firms specializing in application security for independent third-party evaluation.

3 Must provide any non-.gov hostnames being used to CISA and General Services Administration (GSA).

4 Work towards employing immutable workloads when deploying services, especially in cloud-based infrastructure.

(f) Remote Access and Telework Security

1 All remote access must be authenticated via two-factor authentication (e.g., PIV, YubiKey, Fast IDentity Online (FIDO)) where one of the factors is provided by a device separate from the computer gaining access.

2 Use agency-approved tools, including but not limited to chat and video conferencing platforms, within DOE, as applicable.

3 Only use agency-approved methods to share files within DOE, maintaining awareness of distribution and

dissemination, even when utilizing agency-approved platforms.

4 Must follow NIST SP 800-63, *Digital Identity Guidelines*, to ensure a remote connection is automatically logged off after 12 hours.

5 Must use only PIV cards that have been safeguarded and not left unattended without being secured.

6 Access to DOE resources is restricted to approved government-furnished equipment (GFE) or other approved solutions, such as virtual desktop infrastructure (VDI). There should be no direct access to DOE resources outside of GFE or other approved solutions.

(g) Least Privilege

1 Systems must be configured so that every program and every user of the system operates using the least set of privileges necessary.

2 System role assignments must be reviewed to validate compliance with principles of least privilege.

(h) Selection of Security and Privacy Controls

1 Select appropriate and applicable security and privacy controls for IT and OT systems, including for systems maintained within security enclaves, outlined in NIST SP 800-53.

a Security controls are administrative, management, operational, assurance, and technical elements established to safeguard the protection needs of an organization or system.

2 The selection of security controls for the system or enclave should be a risk-based assessment tailored to comply with applicable laws, regulations, organizational policies, and processing requirements.

(i) Foreign National Access to Systems. Controlled access by foreign nations to DOE information systems, including information systems or networks operated by contractors under DOE contracts, must prevent unauthorized (intentional or unintentional) access, disclosure, destruction, or modification to the information or the information system.

(2) Awareness and Training.

(a) Workforce Management. Must abide by requirements detailed in DOE O 360.1, *Federal Employee Training*. Further cybersecurity program training requirements are listed below.

1 AO Workforce Requirements:

a Must require selection of AOs and Authorizing Official Designated Representatives (AODRs) that are experienced, are eligible to obtain national security clearances as appropriate, and have cybersecurity-relevant training or experience.

b Must require that AOs receive initial training on the role and risk-management responsibilities of an AO and refresher training at a specified periodicity.

c AOs (or their delegate, i.e., AODR) must complete the DOE AO training within 60 days of assignment to the position and annually thereafter for the duration of their designation. Upon completion, each AO (or AODR) will receive completion certification from DOE OCIO.

d All AOs must be Federal employees.

2 General initial and annual refresher training must be completed for unprivileged and privileged users.

3 Curriculum is developed and maintained that addresses initial, refresher, and continuing professional development training utilizing NIST's National Initiative for Cybersecurity Education (NICE) work-role based training and development for federal cyber professionals.

4 Specific, role-based training must be provided. This can include:

a CIO, CISO, and AO roles.

b Privacy roles for managing PII.

5 An active anti-phishing program must be in place. Phishing exercises must be held no less than on a quarterly basis.

(3) Data Security.

(a) Data.

1 If technically feasible, all data, including on cloud-based systems, must be encrypted at rest and in transit to the maximum extent possible. Data at backup locations and redundant sites must also be encrypted where feasible.

2 CUI should be prioritized for additional protections. As technology becomes available, DEs and local sites should utilize automated data categorization to identify CUI and automate responses to unauthorized access.

3 Inventory active cryptographic systems, with a focus on HVAs and high impact systems, as outlined in OMB M 23-02, *Migrating to Post-Quantum Cryptography*.

4 To support security operations activities, configure information systems to log, as applicable, all relevant events (examples include but are not limited to Virtual Private Network (VPN), firewall, intrusion detection/prevention systems, network, Endpoint Detection and Response (EDR), and antivirus events).

(4) Information Protection Processes and Procedures.

(a) Information Operations Condition (INFOCON).

1 The DOE CISO must assess the situation and recommend the proper INFOCON level, based on evaluation of all relevant factors.

(b) Insider Threat Program (ITP). The ITP is overseen by the Designated Senior Official of the Office of Environment, Health, Safety and Security (EHSS). Must abide by the ITP requirements, which are outlined in DOE O 470.5.

(c) Vulnerability Disclosure Program (VDP). Attachment 2 sets forth requirements and handling procedures for the Department's VDP.

1 A VDP must be implemented in alignment with OMB M 20-32, *Improving Vulnerability Identification, Management, and Remediation*, and BOD 20-01, *Develop and Publish a Vulnerability Disclosure Policy*, and formalize a mechanism to receive information from external third parties about potential security vulnerabilities

on public facing and internet-accessible DOE systems and websites.

2 Triage and assessment processes must be established for reported vulnerabilities by external third parties.

3 Maintain communication with external third parties on reported vulnerabilities.

4 Track reported vulnerabilities in alignment with risk management and incident reporting metrics and processes.

(d) Social Media Security.

1 Per Department of Homeland Security (DHS) BOD 18-01, *Enhance Email and Web Security*, all publicly accessible DOE websites and DOE web services shall be configured to:

a Provide service through a secure connection (HTTPS only, with HSTS). Secure Sockets Layer (SSL)v2 and SSLv3 shall be disabled on all web servers. Triple Data Encryption Standard (3DES) and Rivest Cipher 4 (RC4) ciphers shall be disabled on web servers and web-based interfaces. These requirements apply to all web-based interfaces, including internally accessible web portals and web-based service interfaces.

b Identify and provide a list of agency second-level domains that can be HSTS preloaded, for which HTTPS will be enforced for all subdomains. This shall be performed annually.

c Prevent or restrict the posting of DOE documents to unapproved or other non-governmental websites.

(e) Vulnerability & Configuration Management.

1 All DOE entities must have established procedures for coordinating responses and reporting for all CISA directed BODs, Emergency Directives (ED), or CISA directed data calls.

2 BOD 19-02, *Vulnerability Remediation Requirements for Internet-Accessible Systems*, must be utilized for informing DOE organizations of identified issues and coordinating

responses including POA&Ms, false positives, and close outs.

3 Inform DOE organizations of catalog updates, coordinate with sites on issues/concerns, and report on site completion of patching and/or mitigations as described in BOD 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities*.

4 Monitor the DOE Continuous Diagnostics and Monitoring (CDM) dashboard, addressing deltas in reporting in CDM versus manual reporting, and coordinating with organizations on any/all outstanding issues as outlined in BOD 23-01.

(5) Maintenance.

(a) Maintenance and repair of DOE assets (on-site or remote) must be performed and logged, with approved and controlled tools in a manner that prevents unauthorized access (in accordance with the System Security Plan).

(6) Protective Technology.

(a) Safeguard portable electronic devices, including removable media, and ensure it is used in a secure manner. Further detailed guidance on portable electronic devices is outlined in Attachment 4.

(b) The requirements for security auditing/logging as defined in OMB M 21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, must be implemented on DOE systems.

d. **NIST CSF Function: Detect**

(1) Anomalies and Events.

(a) Anomalous activity should be detected, and the potential impact of events understood.

1 A baseline of network operations and expected data flows for users and systems shall be established and managed.

2 Detected events should be analyzed to understand attack targets and methods.

3 Event data should be collected and correlated from multiple sources and sensors.

4 Impact of events should be determined.

5 Incident alert thresholds should be established.

(2) Security and Privacy Monitoring.

(a) Continuous System Monitoring.

1 Establish and implement a CDM tool that reports to the DOE CDM dashboard and CISA CDM dashboard.

2 Intrusion detection/prevention systems must be implemented.

(b) Continuous User Monitoring.

1 Implement continuous monitoring of users to maintain situational awareness and identify cybersecurity events.

(c) Visibility and Analytics.

1 Require penetration testing on applicable information systems.

2 Require red team and blue team exercises to be conducted on a frequent basis.

a Determine systems that need red team and blue team exercises and define the appropriate level of frequency for conducting these exercises.

b Conduct these exercises and provide reporting to the AO.

(d) EDR.

1 Implement an EDR solution on all endpoints to increase visibility necessary to respond to cybersecurity threats.

(3) Detection Processes.

(a) Must maintain and test detection processes and procedures to ensure awareness of anomalous events.

(b) Must define roles and responsibilities for detection personnel to ensure they understand and perform their assigned actions and communicate detected event information to appropriate personnel.

(c) Systems must comply with Federal and DOE detection and monitoring requirements as specified in NIST SP 800-53.

(d) Detection process testing must be included during annual incident response testing.

(e) Detection processes must be reviewed and updated annually or when significant changes occur, or problems are encountered with detection activities.

(f) As technology becomes available and is prioritized for implementation in the DE, deploy capabilities such as Data Loss Prevention (DLP) to discover sensitive content and block its exfiltration from the control of the enterprise.

e. **NIST CSF Function: Respond**

(1) Response Planning.

(a) Event and Incident Response.

1 All information systems must have contingency plans and incident response plans and they must be tested annually.

2 DOE CISO ensures there is participation in annual Department-wide cybersecurity incident response exercises.

(b) Incident Handling and Reporting.

1 Report incidents to OCIO-operated Integrated Joint Cybersecurity Coordination Center (iJC3) in accordance with the following:

a Federal Agency incident reporting requirements from OMB and the DHS/CISA, as well as DOE-required reporting guidelines.

b Classified information and incident handling procedures in Department Directives, including DOE O 470.4, *Safeguards and Security Program*.

2 Must define a process for incident reporting that at a minimum adheres to iJC3 reporting requirements, including all cybersecurity incidents involving information or information systems, including privacy breaches, under DOE or DOE contractor control to be identified, mitigated,

categorized, and reported to the iJC3 in accordance with iJC3 procedures and guidance.

3 Must define a process for incident reporting that requires all cybersecurity incidents involving NSS and the loss or unauthorized disclosure of classified information under DOE or DOE contractor control to be identified, mitigated, categorized, and reported to the Officially Designated Federal Security Authority and the Information Assurance Response Center (IARC) in accordance with IARC procedures, including the requirements from DOE O 470.4.

a Incidents involving the loss or unauthorized disclosure of CUI under DOE or DOE contractor control must follow iJC3 (IARC for NNSA) procedures.

4 Must immediately report suspected and/or verified loss of possession, control or physical compromise of Communication Security (COMSEC)/Controlled Cryptographic Items (CCI), actual or suspected technical penetrations (TSCM), and hazards (TEMPEST) to the COMSEC Central Office of Record per CNSS guidance.

(c) Malware.

1 Manage the risk posed by exposure to malware (e.g., viruses, root kits, ransomware, worms) by ensuring incident response plans delineate actions that must be taken in the event of a malware attack. Such actions must at a minimum address detection and analysis activities, how to triage and rebuild systems, and documenting lessons learned.

(2) Communications.

(a) Major Incident Reporting

1 Major incident reporting must abide by the OMB reporting requirements.

2 PII data breach reporting is governed by the breach reporting requirements per OMB M 20-04, *Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements*, and DOE O 206.1.

3 Coordinate incident reporting with the Headquarters Emergency Operations Center (EOC), in accordance with DOE O 151.1, *Comprehensive Emergency Management System*.

(b) Users must immediately report suspected vulnerabilities, security violations, and security incidents to iJC3.

(c) All incidents involving the loss or theft of DOE hardware, software, and/or information in physical form must be reported immediately to iJC3.

(d) OCIO will coordinate with the Office of the General Counsel (GC) to determine the necessity, appropriate process, and means for repairing DOE's reputation after an incident.

(e) For bidirectional reporting, communications, and collaboration between iJC3 and DEs on cybersecurity incidents, the following must be implemented:

1 Maintain a DOE cyber incident dashboard and periodic reporting for leadership, management, cybersecurity professionals, and information resource management operators;

2 Ensure periodic status reporting to governing bodies;

3 Follow formal processes to share lessons learned with DOE to increase situational awareness and improve DOE's collective cybersecurity posture; and

4 Implement processes, platforms, and tools for sharing of cybersecurity threat data within the Department and with relevant Federal Agencies.

(3) Analysis.

(a) Notifications/alerts from detection systems need to be investigated.

(b) Determine the impact of an incident in coordination with other personnel/organizations, as appropriate, during the investigation.

(c) Perform forensics analysis of incidents to support investigations and categorize incidents.

(d) Establish a vulnerability management process for identifying vulnerabilities via internal testing/scanning.

(e) Ensure TSCM personnel are granted access to DOE networks in performance of authorized activities.

(4) Mitigation.

(a) Incident response coordination will be executed by iJC3 and system personnel to prevent expansion of an event, mitigate its effects, and resolve the incident.

(b) System vulnerabilities must be:

1 Remediated or mitigated in accordance with timeframes specified in each DE's respective CSPPs.

2 Included in a POA&M; or

3 Included in an Acceptance of Risk Letter.

(5) Improvements.

(a) Incident response plans must be updated based on lessons learned during incident response or plan testing.

(b) Contingency plans must be updated based on lessons learned during responses to disasters, other events invoking the contingency plan or plan testing.

(c) Incident response strategies must be reviewed and updated, if necessary, at least annually to address system/organizational changes and problems or issues encountered while responding to incidents or plan testing.

(d) Leverage automation and orchestration to improve security response. Employ methods to advance automation of security monitoring and enforcement.

f. **NIST CSF Function: Recover**

(1) Recovery Planning.

(a) Recovery plans should be part of a system's contingency planning process and tested as part of the annual cybersecurity incident response exercise. Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.

(b) Contingency Planning.

1 Establish, maintain, and effectively implement contingency plans and continuity of operations planning for emergency response, alternate processing and storage sites, backup operations, and post-disaster recovery for DOE information systems to ensure the availability of critical IT and OT resources and continuity of operations in emergency situations;

a All continuity of operations (COOP) systems must adhere to the requirements of this Order. Contingency Planning must align with continuity planning and the Department's COOP to better inform risk analysis and risk mitigation and ensure restoring of IT services in accordance with the biennial Business Process Analysis (BPA) and follow on Business Impact Analysis (BIA) of systems, including consideration of those providing or supporting Primary and Mission Essential Functions (PMEFs/MEFs), in accordance with DOE O 150.1, *Continuity Programs*.

2 Identify and maintain essential records dealing with emergency operations and the legal and financial rights of DOE and persons directly affected by DOE actions; and

3 Complete testing of and training on critical information systems which feed continuity operations in accordance with DOE O 150.1 and in coordination with the Office of Primary Interest for that Order, the Office of Emergency Management (NA-40).

(c) Restoration activities must be coordinated with internal and external parties (e.g., coordinating centers, Internet Service Providers (ISP), owners of attacked systems, victims, other computer security incident response teams (CSIRTs), and vendors).

1 For PII/protected health information (PHI) victim notification, refer to DOE O 206.1.

(2) Improvements.

(a) As part of a system's contingency planning processes, ensure recovery planning and processes are improved by incorporating lessons learned into future activities.

(3) Communications.

(a) Recovery activities must be communicated, in accordance with the CISA Cybersecurity Incident & Vulnerability Response Playbooks.

(b) Communication Security (COMSEC) Materials.

1 COMSEC materials and safeguarding requirements to include equipment, installation, reporting, audits, inspections, and training must be handled in accordance with the direction of the DOE COMSEC Central Office of Record (COR).

2 Coordination and any deviations involving COMSEC requirements must come from the DOE COMSEC COR to the appropriate National Authority.

3 Must follow COMSEC requirements/activities as outlined in DOE O 470.6 and coordinate with EHSS regarding Telecommunication and COMSEC activities.

4 The DOE CIO will maintain COMSEC materials and safeguarding requirements to include equipment, installation, reporting, audits, inspections, and training.

5. RESPONSIBILITIES.

a. Deputy Secretary (S2).

(1) Serves as the S1's designee in executing Head of Agency responsibilities for cybersecurity required by Federal law, regulation, or policy in accordance with delegations identified the Secretary's Delegation to the Deputy Secretary.

(2) Accountable to the S1 for providing information security protections commensurate with the risk and magnitude of harm to DOE's operations and assets, individuals, other organizations, and the Nation.

(3) Establishes cybersecurity accountability and provides active support and oversight of monitoring and improvement for the DOE Cybersecurity Program.

(4) Establishes the organizational commitment and the actions required to effectively manage cybersecurity and privacy risk and protect the missions and business functions carried out by DEs consistent with Federal policies, procedures, standards, and guidelines.

(5) Ensures that:

(a) Information security management processes are integrated with Department-wide strategic, operational, and budgetary planning processes.

(b) HDEs provide information security for the information and systems that support the operations and assets under their control.

(c) The Department has adequately trained personnel to assist in complying with cybersecurity requirements in legislation, executive orders, policies, directives, instructions, standards, and guidelines; and

(d) Senior agency officials and all personnel are held accountable for carrying out their responsibilities and complying with the Department's Cybersecurity Program.

(6) As new threats or vulnerabilities are encountered, the S2 may direct the Department to undertake timely remedial measures to protect DOE information, systems, and mission delivery from harm. Through the distributed federated nature of the Department, DEs are responsible for ensuring that appropriate actions are taken.

b. National Nuclear Security Administration (NNSA) Administrator.

(1) Retains overall responsibility and accountability for the NNSA Cybersecurity Program, which includes ensuring the development and maintenance of an NNSA Baseline Cybersecurity Program.

(2) Oversees protection of National Security Systems (NSS) within NNSA purview.

c. Heads of Departmental Elements (HDEs).

(1) Have overall responsibility for the DE-CSPP, and ensure it is implemented in a manner that cost-effectively mitigates risk. All DEs must be covered by a CSPP, which may be developed and maintained by the DE/Site or implemented by adoption of another DE's CSPP based on organizational structure, shared services, or mission needs. HDEs are to manage DE-CSPPs in coordination through governing bodies at the direction of S2 and review and update their DE-CSPP annually based on E-CSPP updates.

(2) Use a risk-based and tailored approach to implement and flow down the requirements and responsibilities of this Order to all subordinate organizational levels through the CSPPs.

(3) Consult, inform, and coordinate with the DOE CIO to resolve cross-DE issues regarding CSPPs.

(4) Incorporate information security into business processes aligned to Federal and Departmental requirements and in consideration of mission needs.

(5) Ensure roles and responsibilities within their DE are identified to implement this Order.

(a) Designate AOs for all DOE component information systems and define any further delegation within the DE.

1 Ensure that standards are maintained for AO qualifications, initial and refresher training, and continuing professional development.

2 Ensure that AOs are appointed for all DOE component information systems and associated personnel are adequately trained and certified in order to perform the tasks associated with their responsibilities.

(b) Designate other Senior Agency Officials (SAOs) to carry out the required tasks to implement this Order.

(6) Lead the development and implementation of the Department's Cybersecurity Risk Management Strategy for their DE/Site, ensuring it aligns with NIST SP 800-37.

(7) Establish and document the organizational tolerance for risk and communicate the risk tolerance throughout the organization including guidance on how risk tolerance influences ongoing decision-making activities.

(8) Ensure that sensitive data, such as PII is appropriately protected both at rest and in transit within, across, and external to the DE's IT and OT systems and networks.

(9) Participate in and support execution of the VDP with overall responsibility for the remediation of vulnerabilities reported on systems and services deemed to be in-scope for the program.

(10) Ensure processes are in place to report cybersecurity and privacy incidents.

(11) Ensure that security assessments are conducted and documented, as applicable, based on their ATO requirements.

(12) Ensure that general unprivileged and privileged users are completing initial and annual refresher training, and that role-based training is provided.

(13) Oversee the management of DOE systems under their purview.

(14) Ensure tracking of performance measures and goals established by OCIO.

(15) Ensure that INFOCON procedures are developed based on CISO requirements and guidance.

d. DOE Chief Information Officer (CIO).

(1) Carries out the responsibilities of the Federal Agency CIO as required by Federal law, regulation, and policy, and is responsible for:

(a) Designating a Senior Agency Information Security Officer (SAISO)/CISO and Enterprise AO.

(b) Reporting to the S1, S2, and governance bodies on the effectiveness of the Department's Cybersecurity Program, including progress of remedial actions.

(2) Serves as the HDE for the purposes of cybersecurity described in this Order for IT and OT services provided by OCIO to other DEs/Sites. This authority may be further delegated. The CIO as HDE for IT and OT services provided to other DEs/Sites documents and communicates to other DEs/Sites the scope covered by the CIO.

(3) Under Federal Information Technology Acquisition Reform Act (FITARA) responsibilities, coordinates Department-wide cybersecurity acquisition, budget, and human capital activities, to include:

(a) Working with DOE Management and Administration and the Department's Senior Procurement Executive to address matters including risk management for IT and OT investments, cybersecurity training, and the review and approval of all Department cybersecurity acquisition/procurement activities. Activities include leveraging GSA contracts and services in obtaining the necessary cybersecurity products and services.

(b) Working with DOE's Office of the Chief Human Capital Officer to align Federal cybersecurity workforce coding with NIST's NICE Framework; identify and report on cybersecurity work roles of critical need; maintain and improve processes for recruitment and hiring based on Departmental needs; and approve all Department officials with the title of CIO or who function in the capacity of a CIO.

(c) Working with DOE's Office of the Chief Financial Officer to review and approve the Department's Federal IT and OT and Federal cybersecurity budget, to include any reprogramming of funds for these items.

(4) Serves as the designee or delegates other required Senior Accountable Official roles related to cybersecurity as approved by S2.

e. DOE Chief Information Security Officer (CISO).

(1) Carries out the SAISO responsibilities required by Federal law, regulation, and policy. Works with DE CISO (or equivalent position) to administer agency responsibilities of FISMA.

(2) Oversees the Department's Cybersecurity Program and its cybersecurity activities as primary responsibilities and leads an office with the specific mission and resources to assist the Department in achieving trustworthy, secure information systems as required by Federal law, regulation, and policy.

(3) Oversees the development and maintenance of cybersecurity policies, procedures, and control techniques to address information security requirements.

(4) Supports the development and execution of the E-CSPP and ensures it is reviewed and updated annually or if a major change occurs within the environment.

(5) Serves as the Enterprise AO. Maintains a register of the DOE's AOs and serves as the primary liaison for the CIO to the Department's AOs, SOs, and information system security officials.

(6) Makes informed enterprise-level cybersecurity risk decisions by developing processes to manage the Department's risk assessments and incorporating qualitative and quantitative approaches to mature into latest industry risk approaches.

(7) Provides flexibility to tailor cybersecurity protections based on risk assessments to manage information security.

(8) Oversees personnel with significant responsibilities for cybersecurity and ensures that the personnel are adequately trained.

(9) Assists HDEs (or their designated representative) with their cybersecurity responsibilities, including to ensure that:

(a) Information systems and common controls Department-wide are covered by approved information security plans and possess current, risk-calibrated authorizations.

(b) Cybersecurity-related activities required across the Department are accomplished in an efficient, cost-effective, and timely manner, and there is centralized reporting of cybersecurity-related activities.

(c) Determination is made for the allocation of resources dedicated to the protection of systems supporting the organization's missions and business functions based on organizational priorities.

(10) Shares effectiveness of the Department's Cybersecurity Program, including progress of remedial actions, to the DOE CIO.

(11) Provides intra-agency and interagency coordination to address cybersecurity requirements of Federal law, regulation, and policy, and is responsible for:

(a) Developing the DOE cybersecurity threat statement in coordination and consultation with IN, EHSS, Office of Cybersecurity Energy Security and Emergency Response (CESER), and NNSA.

(b) Coordinating, implementing, and managing a Department-wide cybersecurity incident reporting, assessment, and response program.

(c) Directing cybersecurity incident management in coordination with other DEs/Sites, and other U.S. Government organizations as circumstances warrant, consistent with the standards and guidelines issued by DHS and OMB.

(d) Coordinating with the DOE CIO/Senior Agency Official for Privacy (SAOP) and Chief Privacy Officer (CPO) to ensure coordination between privacy and information security programs.

(e) Coordinating and developing the Department's response for all agency-level cybersecurity inquiries, FISMA reporting, and other responses to Congress, DHS, and OMB.

(f) Carrying out the Senior Accountable Official for HVAs responsibilities.

(g) Serving as the Agency lead for Information Communications Technology (ICT) C-SCRM. Ensuring cybersecurity and SCRM considerations are integrated into programming, planning,

budgeting cycles; enterprise architectures; the System Development Life Cycle (SDLC); and acquisition.

(h) Serving as the subject matter expert point of contact for the CIO with the HDE and other Federal agencies regarding cybersecurity activities.

(i) Proactively providing applicable threat information to HDEs and other U.S. Government officials.

(12) Establishes and maintains DOE Cybersecurity Data Repository for key cybersecurity information. The Data Repository facilitates enterprise visibility and bi-directional information flows on key items for effective cybersecurity operations.

(13) Issues non-binding amplification guidance to support DEs in developing their DE-CSPPs and may include templates and standard operating procedures (SOPs).

(14) Oversees the development and usage of the CDM program to implement continuous monitoring to maintain situational awareness and identify cybersecurity events.

(15) Oversees the development and implementation of POA&M processes to correct deficiencies and reduce or eliminate vulnerabilities in DOE information systems.

(16) Manages and maintains the operation of the iJC3 to ensure the Department meets Federal agency incident reporting requirements. Ensures the iJC3:

(a) Conducts routine exercises (including incident response), tool training, and threat modeling/reporting.

(b) Investigates alerts from available network sensors, cyber threat intelligence sources, site submitted incident reports to analyze events and understand attack vector trends.

(c) Provides malware sandbox capability for sites to submit samples for automated analysis.

(d) Coordinates reporting and response of incidents and breaches involving PII with the Chief Privacy Officer.

(e) Updates incident response plans based on lessons learned during incident response or plan testing.

(f) Establishes a vulnerability management process for identifying vulnerabilities via internal testing scanning in accordance with the Vulnerability Disclosure Program.

(g) Provides cyber defense recommendations to DOE enterprise organizations when available.

(h) Oversees that timely and relevant cyber defense information is shared throughout the enterprise through automated and standardized means.

(i) Provides enterprise access to an incident response to support sites in case of a significant event requiring additional support.

(j) Manages the DOE Protective DNS tenant providing technical and policy actions to support enterprise wide and site specific Allow and Block actions.

(k) Maintains SOPs that align with CISA Federal Incident Notification Guidelines and NIST SP 800-61, *Computer Security Incident Handling Guide*.

(l) Advises on INFOCON levels and communicates the level as set by the CISO.

(17) Works with other HDEs and Site Managers to coordinate implementation of the requirements established by the OMB and other Federal Agencies and Organizations with directive authority in cybersecurity.

(a) Establishes, maintains, and improves the Department-wide coordination for effective implementation of Federal cybersecurity programs and initiatives.

(b) Defines security reporting requirements. Establishes the criteria for determining the minimum frequency for control monitoring in collaboration with designated DE/Site representatives.

(c) Develops, tests, and implements plans, procedures, and routine testing of critical or other IT systems to ensure continuity and full operational capacity for Department information systems.

(d) Issues Department-wide guidance pertaining to IT/OT and cybersecurity in the form of memoranda, manuals, guidelines, and similar instruments.

(e) Solicits Department-wide IT/OT and cybersecurity performance data in response to internal and external requirements.

(18) Coordinates with the Office of Technical Security (OTS) Director on DOE cybersecurity matters that directly or indirectly affects the implementation of Technical Standards Program (TSP) including:

(a) Assisting with Departmental response to potential cyber impacts to sites that fall under the TSP.

(b) Assisting appropriate Program Offices in developing remediation strategies consistent with federal law and Departmental risk management strategies.

(c) Coordinating with DOE OTS to facilitate exchange of information specific to threats, vulnerabilities, and incident-related information to information systems with the appropriate organizations.

(d) Identifying sources of cyber threat information and a process for sharing the information, as appropriate.

(e) Assisting with representation of the Department's cybersecurity position as it relates to the TSP including official representation or responses to Other Government Agencies (OGAs) on cybersecurity issues related to CIO authorities.

(f) Alerting the Director OTS of potential cyber issues that may impact technical security and operations. Assist in developing remediation strategies consistent with federal regulation and departmental risk management strategies.

(g) Coordinating with GC to determine the necessity, appropriate process, and means for managing public information regarding an incident.

(h) Providing support to TSP activities as required in the TSP Order.

(i) Coordinating between OTS and OGAs for cyber related issues affecting TSP activities.

(19) Incorporates lessons learned into future activities as part of a system's contingency planning processes.

(20) Develops baseline requirements and guidance for INFOCON procedures.

(21) Coordinates and has awareness on INFOCON across all DEs.

f. Chief Risk Officer. Provides counsel and guidance for aligning information security and privacy risk management processes with strategic, operational, and budgetary Departmental planning processes and within the context of management of other Departmental risks.

g. DE/Site CIOs and CISOs. Perform the duties attributed to the DOE CIO and DOE CISO for their respective DEs/Sites as supplemented by their HDE's organizational, regulatory, business and mission requirements.

h. Authorizing Officials (AOs). The AO is a Federal senior official or executive responsible for ensuring that risk associated with information systems are managed appropriately with the authority to formally assume responsibility and accountability for operating an information system; ensuring common controls inherited by organizational systems are appropriate and effective; or using a system, service, or application from an external provider.

(1) Ensure the information security risk to organizational operations, organizational assets, and individuals is managed at an appropriate level, and accept residual risk when necessary and appropriate.

(2) Official with oversight of M&O operations.

(3) Approve plans, memoranda of agreement or of understanding, and POA&Ms, and determine whether significant changes in the information systems or environments of operation require reauthorization.

(4) Accountable to their HDEs for ensuring that information systems under their purview are operated at an acceptable level of risk, which must be documented and communicated to the appropriate officials.

(5) Oversee that existing systems retain ATO until reauthorization is required and ensures the ATO process is followed per the requirements of this Order and the DE-CSPP.

(6) Ensures that appropriate protections are in place to safeguard sensitive data within, across, and external to information systems and networks.

i. System Owners. Have budgetary oversight for the system or are responsible for the mission and/or business operations supported by the system.

(1) Ensures Authorization Process applies to FISMA systems.

(2) Ensures systems comply with Federal and DOE detection and monitoring requirements.

j. Information Systems Security Officers (ISSO). Ensures implementation of adequate system security and policies in order to prevent, detect, and recover from security breaches and reduce the level of risk. An ISSO must be assigned by the AO for every Federal information system.

(1) M&O must appoint an ISSO for a contractor-operated information system.

k. Chief Acquisition Officer/Cognizant Senior Procurement Executive. Advises and assists Departmental officials to ensure that mission is achieved through the management of acquisition activities. They are essential partners in SCRM efforts.

l. Heads of Contracting Activities. Overall responsibility for managing contracting activities.

m. Contracting Officers (COs). Once notified of contract applicability, incorporate the CRD into M&O contracts, and non-M&O contracts.

n. Cybersecurity/Risk Governance Bodies. Boards and Councils established by senior officials that advise the Department's senior decision makers. HDEs coordinate and collaborate on IT and OT risk management and cybersecurity matters through a DOE CIO-chaired subject matter expert-level governance body that reports to a primary policy governance body chaired by the S2. See charters referenced in the References Attachment.

o. Director of the Office of Intelligence and Counterintelligence (IN).

(1) Serves as the AO for DOE information systems under the purview of the Intelligence Community. This authority may be further delegated. The delegating official remains responsible and accountable.

(2) Ensures that intelligence systems operated by Headquarters and Field Elements of the Office of Intelligence and Counterintelligence are protected in accordance with applicable Director of National Intelligence and DOE policy and directives.

p. Director of the Office of Enterprise Assessments (EA). Provides independent oversight of the DOE Cybersecurity Program in accordance with the mission, functions, and assigned responsibilities of the Office of Enterprise Assessments and associated national requirements and DOE directives.

q. Director of Environment, Health, Safety and Security (EHSS).

(1) Sets the physical and technical security policy, especially for the introduction and use of controlled articles (such as information systems) and technical security requirements and countermeasures.

(2) Manages the DOE COMSEC COR and is the Command and Controlling authority for COMSEC material and controlled cryptographic item (CCI) equipment for the Department.

6. INVOKED STANDARDS. This Order does not invoke any DOE technical standards or industry standards as required methods. Any technical standard or industry standard that is mentioned in or referenced by this Order is not invoked by this Order. Note: DOE O 251.1D, Appendix J provides a definition for "invoked technical standard."

7. REFERENCES. Attachment 5 provides published laws, rules, regulations, policy, directives, standards, guidance, and other issuances cited and additional information sources to assist in implementing this Order.

8. DEFINITIONS. Attachment 6 provides definitions and acronyms.

9. CONTACT. Questions concerning this Order should be directed to the Office of the Chief Information Officer at (202) 586-0166.

BY ORDER OF THE SECRETARY OF ENERGY:

DAVID M. TURK
Deputy Secretary

ATTACHMENT 1
CONTRACTOR REQUIREMENTS DOCUMENT (CRD)
DOE O 205.1D, *DEPARTMENT OF ENERGY CYBER SECURITY PROGRAM*

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 (GO-CO) systems are subject to DOE CRD standards and requirements.

In addition to the requirements set forth in this CRD, contractors are responsible for complying with the Attachments (Vulnerability Disclosure Program (VDP) Policy and Handling Procedures, National Security Systems (NSS), Portable Electronic Device Security) to DOE O 205.1D, referenced in and made a part of this CRD, which provides information and requirements applicable to contracts in which this CRD is inserted. All applicable guidance and requirements from Executive Orders (EOs), Committee on National Security Systems (CNSS) Issuances, Office of Management and Budget (OMB) Memorandums, Binding Operational Directives (BODs), and National Institute of Standards and Technology (NIST) Publications are to be followed in accordance with DOE O 226.1, *Implementation of Department of Energy Oversight Policy*.

External references and policies must follow Departmental Element (DE)/Contracting Officer (CO) and contractor assurance mechanism or process before compliance is mandated, regarding new or changes in external references and policies.

1. GENERAL REQUIREMENTS. The contractor must:

   a. Govern

      (1) Establish a Cybersecurity Program Plan (CSPP) that is consistent with the requirements provided by the applicable Departmental Element guidance.

      (2) Incorporate Federal initiatives as directed by the Contracting Officer (CO) where mission appropriate, or where required in the E-CSPP and/or DE-CSPP.

      (3) Abide by E-CSPP and/or DE-CSPPs through contracting processes described in this Order or by inheritance/adoption of E-CSPP and/or DE-CSPP for Federal sites.

      (4) Management and Operating (M&O) must appoint an Information Systems Security Officers (ISSO) for a contractor-operated information system.

   b. Identify

      (1) Provide and maintain key cybersecurity information for the DOE Data Repository as requested.

(2) In coordination with local sites, comply with DHS CISA BODs and EDs as applicable, to include BOD 23-01, *Improving Asset Visibility and Vulnerability Detection on Federal Networks*.

(3) Abide by High Value Assets (HVA) requirements as detailed in OMB M 19-03.

(4) Ensure all information systems operate within the processes defined and approved by the Federal Authorizing Official, and that all systems maintain a documented acceptable level of risk pursuant to (1) the agreed-on risk profile defined by Site and Federal management, (2) approved oversight and assurance systems, and (3) approved ATO prior to operating.

(5) Ensure records contained in an information system are managed in electronic format in accordance with an authorized federal records schedule and DOE O 243.1, *Records Management Program.*

(6) Assess and manage risk within their environment, in the context of acceptable mission risk set collaboratively with the Federal Site Manager.

c. Protect

(1) Establish and maintain a zero-trust architecture (ZTA) plan in alignment with the DOE enterprise and network.

(2) 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.

(3) Support protection and maintenance of DOE data and systems in accordance with the applicable E-CSSP and/or DE-CSPP.

(4) Establish and maintain a process to support VDP for vulnerabilities reported to in-scope DOE websites and systems.

(5) Must ensure that security specifications and requirements are included in procurements of IT and OT systems and components.

(6) Ensure all contractors and subcontractors have policies that address supply chain management, System Development Life Cycle (SDLC) and Software Bill of Materials as noted in NIST SP 800-161.

d. Detect

(1) Establish a process to ensure that users acknowledge and consent to privacy and monitoring policies.

(2) Establish and manage a baseline of network operations and expected data flows for detecting any anomalous activity and ensure the potential impact of events is understood.

e. Respond

(1) Establish and maintain an effective Assurance System that provides metrics of the overall performance and appropriate transparency to federal oversight at the local DE/Site level regarding cybersecurity risk management and overall performance.

(2) Establish and maintain an Incident Management Handling and Reporting Capability that is consistent with the contractor requirements contained within the applicable E-CSPP and/or DE-CSPP.

f. Recover

(1) Develop and manage recovery processes and procedures to ensure restoration of systems or assets affected by cybersecurity incidents. The developed recovery processes must be tested annually or if a major change occurs within the environment.

(2) Implement contingency planning and continuity of operations for contractor-ran systems on behalf of federal oversight at the local level.

(3) Implement contingency planning and continuity of operations for emergency response in accordance with DOE O 150.1, *Continuity Programs*.

(4) Implement contingency planning and continuity of operations for HVAs.

ATTACHMENT 2
VULNERABILITY DISCLOSURE PROGRAM (VDP)
POLICY AND HANDLING PROCEDURES

This Attachment provides information and/or requirements associated with DOE O 205.1D as well as information and/or requirements applicable to contracts in which the associated CRD (Attachment 1 to DOE O 205.1D) is inserted.

This Vulnerability Disclosure Program: Requirements and Handling Procedures supports the Department of Energy's (DOE) Cybersecurity Program and meets the requirements of the Office of Management and Budget (OMB) Memorandum (M) 20-32, *Improving Vulnerability Identification, Management, and Remediation* and the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Binding Operational Directive (BOD) 20-01, *Develop and Publish a Vulnerability Disclosure Policy*. This Attachment will enhance the cybersecurity posture of the DOE through the development of a formal mechanism to receive information from members of the public acting in good faith (hereafter referred to as Reporters) about potential security vulnerabilities on DOE websites, systems, or digital services that are within scope of this program or are internet-accessible through a publicly routed internet protocol (IP) address or a hostname that resolves publicly in Domain Name System (DNS) to such an address. This includes DOE web-based forms, web-based applications, and digital services.

A Reporter is defined as any person or entity external to the Department, who or which in good faith submits a security vulnerability or vulnerabilities to the Department consistent with this Attachment. The handling procedures provided herein codify the DOE's process for receiving, evaluating, and remediating potential vulnerabilities, facilitate transparency and communication between DOE and the public, and set out minimum requirements for Departmental Elements, program offices, and associated sites.

1. REQUIREMENTS.

   a. Scope. Office of the Chief Information Officer (OCIO), in alignment with applicable laws and directives, will determine the overall scope of this Attachment and will work with Heads of Departmental Elements (HDEs) to determine which systems and services are under their purview. The scope of the Attachment shall progressively expand such that:

      (1) At the issuance of this Attachment, the DOE OCIO has identified at least one DOE website, system, or digital service produced for public use or that is internet-accessible to be in-scope.

      (2) At the issuance of this Attachment, all newly launched and produced DOE websites, systems, or digital services intended for public use or made internet-accessible hereafter will be considered in-scope under the Attachment.

      (3) Within 270 calendar days after the issuance of this Attachment, and within every 90 calendar days thereafter, the scope of this Attachment will

increase by at least one DOE website, system, or digital service intended for public use or made internet-accessible.

(4) At two years after the issuance of this Attachment, all DOE produced websites, systems, or digital services intended for public use or made internet-accessible will be in-scope of this Attachment.

b. Out of Scope Systems and Services. The following websites, systems, and services are excluded from the testing provisions and legal protections afforded to Reporters within this Attachment. If Reporters are uncertain of whether a website, system, or digital service is in-scope of this Attachment, it is recommended that they contact the designated security point of contact to confirm.

(1) National Security Systems (NSS), the definition for a National Security System, along with other applicable terms used in the National Security Community, are found in CNSSI 4009, *Information Assurance Glossary*.

(2) Websites, systems, and digital services owned by Third Party Service Providers. The DOE uses third-party services to assist the Department in communicating or interacting with the public. These services may be completed using separate websites, systems, and digital services or may be embedded in DOE produced websites, systems, and digital services. DOE information maintained and operated by Third Party Service Providers, or websites, systems, and digital services owned by Third Party Service Providers but operated or controlled by the Department are subject to the provider's privacy policies. Testing of such websites, systems, or digital services is not protected under this Attachment.

(3) Non-Public Facing or non-Internet-accessible websites, systems, and digital services.

c. Policy. The Department's Vulnerability Disclosure Program serves to enhance the resiliency of the Department's internet-accessible systems and services by providing an authorized disclosure process for Reporters to report potential security vulnerabilities or issues. Reporters who make a good-faith effort to follow this Attachment and its corresponding rules of engagement enable the DOE to reduce risk to its infrastructure by incentivizing coordinated disclosure to remediate vulnerabilities with expediency. A security vulnerability means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control. Controls can be viewed as descriptions of the safeguards and protection capabilities appropriate for achieving the particular security and privacy objectives of the organization and reflecting the protection needs of organizational stakeholders. The following actions are required to facilitate the intake, review, and remediation of reported security vulnerabilities and ensure communication between the Department and Reporters.

(1) Process to Submit a Vulnerability Report.

(a) A Reporter may submit an identified potential vulnerability or vulnerabilities to the Department via doe.responsibledisclosure.com. Information submitted via this portal will be encrypted in transit and at rest, and anonymized to protect the identity of the Reporter;

(b) The Reporter must accept the terms and conditions before submitting a security vulnerability. All submissions will be subject to relevant federal disclosure statutes including 5 U.S.C. § 552, *Public information; agency rules, opinions, orders, records, and proceedings*, although the anonymity of the report will be protected as required by this Attachment and Federal law. Following acceptance of the terms and conditions, the Reporter will provide detailed information about the security vulnerability to enable DOE to replicate the discovery of the vulnerability, including all relevant details such as product(s), version(s), and configuration setting(s);

(c) The iJC3 will validate the credibility of all reported security vulnerability submissions using the Common Vulnerability Scoring System (CVSS) or other approved methodology and prioritize for remediation action as necessary. Validation may entail collaboration with the Reporter to obtain additional information necessary to analyze the reported security vulnerability. The Reporter will not be required to produce or share any personally identifiable information (PII) during this process; and

(d) Reporters are encouraged to assess the potential impact of the vulnerability they are submitting via Common Vulnerability Scoring System (CVSS) or other similar methodology in order to ensure that only high-impact vulnerabilities are disclosed.

(2) The following types of research testing methods are prohibited from being used in good-faith to identify potential security vulnerabilities on DOE internet-accessible systems and services within scope of this Attachment and are in violation of the Department's Vulnerability Disclosure Program:

(a) No security testing is authorized on industrial control systems (ICS) managed by DOE, but reports of information security concerns on ICS are accepted and will be elevated for remediation as required.

(b) Denial of Service testing.

(c) Physical or social engineering (e.g., phishing).

(d) Methods that disrupt system operation or result in the modification or destruction of data.

(e) Exploitation of a vulnerability beyond the minimal amount of testing required to prove that a vulnerability exists or to identify an indicator related to a vulnerability.

(f) Any other activity that would not reasonably be considered prudent given the terms, conditions, and intent of this Attachment.

(3) In addition, Reporters shall not:

(a) Conduct data exfiltration.

(b) Intentionally compromise the privacy, safety, intellectual property (IP), or other commercial or financial interests of any DOE employee, contractor, or DOE-associated entity.

(c) Intentionally compromise any Controlled Unclassified Information (CUI), including PII and IP, or Official Use Only (OUO) information.

(d) Retain or transmit any information, including PII or IP, belonging to the Department.

(e) Request monetary compensation for time, materials, expenses, and effort (e.g., a bounty) or a property interest of any type or kind for any security vulnerabilities that they may discover.

(4) The Department will acknowledge Reporter receipt of each vulnerability within three business days of submission. Acknowledgement to the Reporter may be, but is not limited to, a notice published on a Department-approved website/portal indicating the status of the submitted vulnerability. The Reporter may also choose to remain anonymous. The Department will be as transparent as possible about what steps it is taking during the remediation process.

(5) DOE requests that Reporters not publicly disclose a security vulnerability or vulnerabilities prior to the time-limited response period as determined by DOE.

(6) The Department will not recommend or pursue legal action against anyone for a security-reporting activity that the Department concludes represents a good-faith effort to follow the Attachment and will deem that activity authorized.

d. Publication of Vulnerability Disclosure Program. At the issuance of this directive, DOE will publish the Attachment as a web page in plain text or HTML.

e. Security File. At the issuance of this Attachment, DOE will create a security.txt file at the doe.gov domain.

2. VULNERABILITY DISCLOSURE HANDLING PROCEDURES.

a. The following handling procedures are requirements to support the effective implementation of this Attachment:

(1) Receipt and Tracking. All reported vulnerabilities will be tracked to conclusion using the following steps:

(a) Vulnerability reports will be tracked from when a report is first received up to its resolution via the vulnerability disclosure portal;

(b) Vulnerability reports will be available to system owners within 48 hours of submission, and a channel will be established for the system owners to communicate with vulnerability Reporters, as appropriate;

(c) When a vulnerability report is submitted via the vulnerability disclosure portal, it will be triaged by iJC3 based on the potential impact to system confidentiality, integrity, or availability and assigned a score based on the CVSS or other accepted methodology; and

(d) Reports of vulnerabilities requiring remediation will be transmitted to the appropriate system or service owner via the iJC3.

(2) Remediation. Upon receipt of a verified vulnerability from the iJC3, the system or service owner will remediate the vulnerability and document actions taken or provide documentation of risk acceptance. The owner should then determine if this verified vulnerability has ever been previously exploited or if there have been prior attempts to exploit this vulnerability. DOE will adhere to DHS-published timelines for vulnerability remediation, as applicable.

(3) Incident Investigation and Remediation. If an investigation determines that a vulnerability reported via the Vulnerability Disclosure Program was exploited prior to its discovery, an incident report will be opened. Such an incident will be remediated by the system or service owner or supporting incident response team and reported to iJC3 according to the established iJC3 incident reporting requirement.

(4) Out of Scope Systems and Services. If a report is submitted for systems and services that are out of scope, the response to the Reporter should acknowledge the report and inform them that the report falls outside of the scope as described in the Attachment.

(5) Communication. Receipt of each submission will be acknowledged within three business days. Acknowledgement may be, but is not limited to, a notice published on a Department-approved website that identifies the Reporter by name or handle and details the date and time of their submission. Alternatively, the Reporter may elect to remain anonymous in which case the Reporter will not be identified. The following communication procedures will apply for submitted vulnerabilities:

(a) Initial assessment of each vulnerability report will be completed within seven business days from initial submission. The verification team will be responsible for completing the initial assessment of each vulnerability.

(b) Resolution of credible security vulnerabilities, including notification to the Reporter, will occur on a timely basis from initial submission.

(c) Credible reports of newly discovered or not publicly known vulnerabilities on agency systems that use commercial software or services that affect or are likely to affect other parties in government or industry, as well as vulnerabilities requiring inter-agency support, will be reported immediately to the Cybersecurity and Infrastructure Security Agency.

(6) Compliance and Noncompliance with Attachment. The Department will not take civil action or bring a complaint to law enforcement for unintentional, good faith violations of this Attachment. If legal action is taken by a third party against a Reporter who complied with the Attachment and the corresponding Rules of Engagement, the Department will take appropriate measures to show that the Reporter's actions were in compliance with the Attachment. It is recommended that Reporters should first contact the iJC3 before testing any internet-accessible system that may be out of the Attachment's scope.

3. RESPONSIBILITIES.

a. DOE Office of the Chief Information Officer (OCIO).

(1) Carries out the responsibilities of the Federal Agency CIO as required by Federal law, regulation, and policy, and is responsible for:

(a) Executing the Attachment in compliance with federal guidelines and requirements.

(b) Defining security vulnerability reporting requirements, including establishing the criteria to determine the systems and services in-scope of this Attachment in collaboration with designated Departmental Elements/Site representatives.

(2) Works with the DOE CISO and HDEs (or their designated representatives) to ensure that:

(a) Applicable systems and services under DOE ownership, use, and control fall within scope of the Attachment.

(b) HDEs provide information and support for the applicable systems and services within scope of this Attachment and ensure that system and service owners execute remediation for vulnerabilities under their authority to use for identifying the scope of the Attachment.

(c) Infrastructure and services necessary to support security vulnerability reporting, tracking, and communication are established and protected.

(d) Validated security vulnerabilities and associated metrics are included in any Agency reporting to DHS, OMB, and other federal entities as necessary.

(e) This Attachment and handling procedures are reviewed every three years to align with federal requirements and to account for changes in the general cybersecurity landscape to incorporate additional best practices to receive, track, and report vulnerabilities identified by Reporters.

b. iJC3.

(1) Reviews reported vulnerabilities for credibility.

(2) Directs reported vulnerabilities to the appropriate system or service owner.

(3) Ensures that system or service owners receive reported vulnerabilities.

(4) Confirms that vulnerabilities have been properly remediated.

(5) Tracks individual vulnerabilities from initial report through remediation.

(6) Communicates with Reporters through all stages of the vulnerability disclosure process.

(7) Collects metrics on vulnerabilities reported under the Vulnerability Disclosure Program, enabling the Department to meet reporting requirements under OMB M-20-32, BOD 20-01, and other applicable directives and laws.

(8) Informs the OCIO with regular reports on the status of vulnerabilities disclosed under the VDP.

(9) Ensures that critical vulnerabilities with the potential to adversely impact the Department's mission are promptly brought to the attention of the OCIO leadership.

(10) Conducts trend analysis on reported vulnerabilities across the enterprise in order to identify opportunities for systematic improvement in the Department's cyber posture.

c. Heads of Departmental Elements (HDEs).

(1) Shall ensure compliance with the Attachment for any in-scope systems and services under their purview and support timely prioritization, communication, and remediation of vulnerabilities reported.

(2) Have overall responsibility for the remediation of vulnerabilities reported on systems and services deemed to be in-scope for the program.

(3) Consult, inform, and coordinate with the DOE CISO to resolve cross-Departmental Element vulnerabilities and issues.

d. Authorizing Officials (AOs). Responsible for the accepting of risk for this Attachment's in-scope systems.

e. System and Service Owners.

(1) Responsible for remediation of credible vulnerabilities reported through the Attachment and meeting all relevant communication and remediation timelines listed herein; and

(2) Shall provide all required documentation of vulnerability remediation or risk acceptance to iJC3.

4. REFERENCES.

a. Office of Management Budget (OMB) Memorandum (M) 20-32, *Improving Vulnerability Identification, Management, and Remediation*, September 2, 2020. This memorandum provides Federal agencies with guidance for obtaining and managing their vulnerability research programs.

b. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Binding Operational Directive (BOD) 20-01, *Develop and Publish a Vulnerability Disclosure Policy*, September 2, 2020. This directive promulgates a requirement for Executive Branch Departments and Agencies to publish a vulnerability disclosure policy.

c. 5 U.S.C. § 552, Public information; agency rules, opinions, orders, records, and proceedings. Created by the Pub. L. 89–554, Sept. 6, 1966, 80 Stat. 383, also known as The Freedom of Information Act, this statute generally requires that

departments and agencies make information on rules, opinions, orders, records, and proceedings available to the public.

d. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 29147:2018 Information technology — Security techniques — Vulnerability disclosure. This document describes vulnerability disclosure: techniques and policies for vendors to receive vulnerability reports and publish remediation information.

e. ISO/IEC 30111:2019 Information technology — Security techniques — Vulnerability handling processes. This document describes processes for vendors to handle reports of potential vulnerabilities in products and services.

f. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.

g. NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).

5. DEFINITIONS.

a. Control. For the purposes of this Attachment, DOE utilizes the definition of the term control as found in NIST SP 500-83, Security and Privacy Controls for Federal Information Systems and Organizations:

(1) Controls can be viewed as descriptions of the safeguards and protection capabilities appropriate for achieving the particular security and privacy objectives of the organization and reflecting the protection needs of organizational stakeholders. Controls are selected and implemented by the organization in order to satisfy the system requirements. Controls can include technical aspects, administrative aspects, and physical aspects. In some cases, the selection and implementation of a control may necessitate additional specification by the organization in the form of derived requirements or instantiated control parameter values.

b. Credible Vulnerability. A reported vulnerability that has been validated by iJC3 and for which remediation steps have been determined by the appropriate system and service owners.

c. Good Faith. An absence of fraudulent or malicious intent, and a desire to help—not harm—the Department.

d. Internet Accessible System. Any DOE system that is reachable over the public internet that has a publicly routed IP address or a hostname that resolves publicly in DNS to such an address. An internet-accessible system is not infrastructure that is internal to the DOE network that enables endpoints to be accessible over the internet, systems reachable from the internet but that require special configuration

or access controls (e.g., via a Virtual Private Network), or shared services used by the Department.

e. Reporter. Any person or entity external to the Department, who or which in good faith submits a security vulnerability or vulnerabilities to the Department consistent with this Attachment. The Department allows that persons or entities other than the one who or that discovered the security vulnerability may come forward and present as the Reporter.

f. Security Vulnerability. For the purpose of this Attachment, DOE utilizes the definition of the term security vulnerability as found in the Cybersecurity Information Sharing Act of 2015, 6 U.S.C. § 1501(17): Security vulnerability means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

g. Vulnerability Disclosure. The "act of initially providing vulnerability information to a party that was not believed to be previously aware."

6. CONTACT. Questions concerning this attachment should be directed to the Office of the Chief Information Officer at (202) 586-0166 or DOEOCIOInfo@hq.doe.gov.

ATTACHMENT 3
NATIONAL SECURITY SYSTEMS (NSS)

This Attachment provides information and/or requirements associated with DOE O 205.1D as well as information and/or requirements applicable to contracts in the associated CRD (Attachment 1 to DOE O 205.1D) regarding the protection and safeguarding of National Security Systems.

1. REQUIREMENTS.

   a. Identifying and Designating NSS.

      (1) All DOE IT and OT that is designated as an NSS must comply with requirements of Committee on National Security Systems (CNSS) and Intelligence Community Directives (ICDs) where applicable.

      (2) Must have processes for designating the appropriate information classification levels to classified NSS (if applicable) from Executive Order 13526 and Title 10 Code of Federal Regulations (CFR) Part 1045 (Confidential, Secret and Top Secret) and determine potential impacts of Low, Moderate and High per CNSSI 1253, Security Categorization and Control Selection for National Security Systems.

      (3) Deployment requirement(s) for Cross Domain Solution (CDS) by contractor should be handled with due care to protect sensitive contractor data; operational realities; and unnecessary exposure of information systems, components, and data. Ensure inventory and maintenance of NSS systems and CDS deployments.

      (4) NIST SP 800-59, Guideline for Identifying an Information System as a National Security System, must be used as guidance for National Security Systems.

   b. Procuring NSS.

      (1) Ensure that security specifications are included in procurements of components for NSSs.

      (2) Warranty clauses must be established for security specifications in procurements of components for NSSs of such duration and coverage sufficient to protect the public interest, after considering items such as risks, complexity of components, and cost (if any).

   c. Safeguarding NSS.

      (1) Implement multifactor authentication and encryption for NSS data-at-rest and data-in-transit. In those instances where the head of an agency determines the agency is unable to implement these measures, the head of

the agency shall authorize an exception pursuant to the process provided in section 3 of National Security Memorandum (NSM)-8, *Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems*.

(2) To ensure widespread cryptographic interoperability among NSS, use NSA-approved, public standards-based cryptographic protocols. If mission-unique requirements preclude the use of public standards-based cryptographic protocols, NSA-approved mission unique protocols may be used. New systems shall not be authorized to operate that do not use approved encryption algorithms and implementations.

(3) As stated in the Requirements section of this order, observe the requirements stated as law, obligation, and/or government-wide policy stemming from governance bodies external to the department, such as other Federal Agencies, Congress, or the White House, including but not limited to the Federal Information Security Modernization Act of 2014 (FISMA), Executive Order (EO 14028), and Binding Operational Directives (BODs).

(4) Protect Restricted Data (RD), Formerly Restricted Data (FRD) and Trans-classified Foreign Nuclear Information (TFNI) on NSS consistent with DOE O 471.6, *Information Security*; DOE O 475.2, *Identifying Classified Information*; and DOE O 452.8, *Control of Nuclear Weapon Data*.

d. Coordinating and Reporting.

(1) Must define a process for supporting reports based on National Manager's request on the overall cybersecurity posture of DOE's NSS. This process must involve the designated Departmental Element point of contact.

(2) Follow all Emergency Directives and National Manager BODs issued by National Manager to take any lawful action with respect to the operation of that NSS, as defined in NSM-8, including such systems used or operated by another entity on behalf of DOE, for the purpose of protecting the NSS from, or mitigating, the threat, vulnerability, or risk.

(3) Upon detection of a known or suspected compromise or otherwise unauthorized access to NSS, report such compromise or unauthorized access through the designated Departmental Element point of contact to the National Manager.

(4) Must define a process for incident reporting that requires all cybersecurity incidents involving NSS and the loss or unauthorized disclosure of classified information under DOE or DOE contractor control to be identified, mitigated, categorized, and reported to the Officially Designated Federal Security Authority and the IARC in accordance with

IARC procedures, including the requirements from DOE O 470.4, *Safeguards and Security Program*.

e. Governance.

(1) Ensure DE-CSPPs include adoption and use of cloud technology and ZTA.

(2) Implement DOE classified data protection levels as defined in their respective DE-CSPPs or applicable system (network) owner/operator requirements and governance. Contractors with NSS must apply the classification markings in the electronic environment as described in the applicable DE-CSPPs.

(3) For Sensitive Compartmented Information systems, DEs must comply with ICDs. The DOE Office of Intelligence and Counterintelligence (IN) approves operation of these information systems.

f. Equivalencies and Exemptions.

(1) Requests for equivalencies and for exemptions from CNSS requirements must follow those processes, as amplified by direction within the applicable DE-CSPP.

(2) The Chief Information Officer (CIO) shall retain internal records regarding system exceptions sufficiently detailed to perform effective and timely identification and mitigation of any cybersecurity issues that may impact these systems.

ATTACHMENT 4
PORTABLE ELECTRONIC DEVICE SECURITY

This Attachment provides information and/or requirements associated with DOE O 205.1D as well as information and/or requirements applicable to contracts in the associated CRD (Attachment 1 to DOE O 205.1D) regarding the management and safeguarding of portable electronic devices. Departmental Elements (DEs) are required to address the following requirements in their Departmental Element Cybersecurity Program Plans (DE-CSPPs) using a risk and performance-based approach. Sites must work with their DE counterparts to (i) identify requirements that align with their local risk assessments and (ii) adopt or adjust those identified requirements in their corresponding CSPP.

1. PORTABLE ELECTRONIC DEVICE MANAGEMENT PROCEDURES. Appropriate device management procedures and oversight processes must be documented and implemented that address:

   a. General Procedures for Portable Electronic Devices that Store or Access DOE Information.

      (3) DE-CSPPs and Site Cybersecurity Plans must adopt a risk-based approach towards the protection of DOE information from unauthorized access. The use of Government Furnished Equipment (GFE), by the Agency or by a Contractor in the performance of a service under a contract with the Agency, that includes the storage of or access to DOE information, must be governed by a set of enforceable controls, policies, and procedures that provide adequate protections. These protections must:

         (a) Align with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 control requirements mapped to the categorization introduced in Federal Information Processing Standards (FIPS) 199;

         (b) Derive from local risk assessments that address threats which may compromise the confidentiality, availability, or integrity of DOE information;

         (c) Allow for policies that adopt a graded risk-based approach towards DOE information storage such that hardware controls scale with the level of sensitive information permitted on the GFE, based on local risk assessments that are informed by the mission of the site;

         (d) Encourage configurations at either the level of the DOE GFE endpoints or at the level of a DOE-owned system that minimizes the risks of using removable media drives on GFE endpoints, based on the categories of information permitted for storage and access on the GFE;

(e) Develop guidance that describes the use of DOE GFE portable devices for incidental non-organizational/personal use to prevent the compromise of DOE Information;

(f) Establish requirements for the encryption of portable GFE devices, including the use of FIPS compliant encryption where indicated.

(g) Require GFE inventory and reporting processes consistent with applicable Property Management requirements.

b. Procedures for Portable Devices for Foreign Travel.

(4) Following the requirements defined in this Order, risk management plans addressing GFE use on foreign travel must be implemented by the Heads of Departmental Elements (HDE). Sites must implement the procedures as laid out in their respective CSPP. DEs that issue GFEs must establish travel procedures to include the following considerations:

(a) Establish a foreign travel pre-departure briefing and risk assessment determination for staff visiting sensitive countries in scope of the approved travel. The briefing should provide guidance on GFE storage and connectivity, as well as reporting procedures for lost devices.

(b) Apply controls that ensure the confidentiality, integrity, and availability of DOE information, regardless of whether GFE or a Personal Device is in use during travel.

(c) Establish risk-based requirements for the use of loaner devices on international travel, based on information about the risks associated with specific countries as determined by the Department of State.

2. BRING YOUR OWN DEVICE (BYOD).

a. If a personal device is used by an employee of the Agency or by a Contractor in the performance of a service under a contract with the Agency, it must be governed by a set of enforceable controls, policies, and procedures that address threats which may compromise the confidentiality, availability, or integrity of DOE Information. Policies and controls must be implemented that adopt a graded risk-based approach towards DOE Information storage such that hardware controls scale with the categories level of sensitive information permitted on the device, based on local risk assessments that are informed by the mission of the site.

ATTACHMENT 5
REFERENCES

This Attachment provides information and/or requirements associated with DOE O 205.1D as well as information and/or requirements applicable to contracts in which the associated CRD (Attachment 1 to DOE O 205.1D) is inserted.

1. FEDERAL LAWS AND REGULATIONS.

   a. 44 United States Code (U.S.C) Chapter 29, Records Management by the Archivist of the United States and by the Administrator of General Services.

   b. Atomic Energy Act of 1954, as amended (Public Law (Pub.L.) 83-703; 42 U.S.C. § 2011 et seq.).

      (1) Note: A violation of the provisions relating to the safeguarding or security of Restricted Data (RD), or other classified information may result in a civil penalty pursuant to subsection a. of Section 234B of the Atomic Energy Act of 1954 (42 U.S.C. 2282b). The procedures for the assessment of civil penalties are set forth in Title 10, Code of Federal Regulations (CFR), Part 824, Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations.

   c. Clinger-Cohen Act of 1996, Pub.L. 104-106.

   d. Cybersecurity Act of 2015, Pub.L. 114-113, enacted 12-18-2015. Federal Information Technology Acquisition Reform Act (FITARA), Pub.L. No. 113–291 Title VII, Subtitle D, Section 831–837 of the National Defense Authorization Act for Fiscal Year 2018, enacted 12-12-2017. Federal Information Security Modernization Act (FISMA) of 2014, Pub.L. 113-283, enacted 12-8-2014.

   e. Department of Transportation and Related Agencies Appropriations Act of 2000, Pub.L. 106-346, §359.

   f. Energy Policy Act of 2005, Pub.L. 109-58.

   g. Federal Risk and Authorization Management Program (FedRAMP) Authorization Act per H.R. 7776, National Defense Authorization Act for Fiscal Year 2023.

   h. High-Performance Computing Act of 1991, Pub.L. 102-194.

   i. Privacy Act of 1974, Pub.L. 93-579.

   j. Telework Enhancement Act of 2010, Pub.L. 111-292.

   k. Title 10 Code of Federal Regulations (CFR) § 1017, Identification and Protection of Unclassified Controlled Nuclear Information.

l. Title 10 CFR § 1045, Nuclear Classification and Declassification.

m. Title 32 CFR § 2001.23, Classification Marking in the Electronic Environment.

n. Title 32 CFR § 2002, Controlled Unclassified Information (CUI).

o. Title 36 CFR § 1236.10, Records Management and Preservation Considerations for Designing and Implementing Electronic Information Systems.

p. Title 36 CFR § 1236.12, Records Management and Preservation Considerations for Designing and Implementing Electronic Information Systems.

q. Title 36 CFR § 1236.20, Additional Requirements for Electronic Records.

r. Title 44 U.S.C. 3542, Information Security Definitions.

2. NATIONAL CYBERSECURITY POLICIES AND GUIDANCE.

a. Executive Order (EO) 12344, Naval Nuclear Propulsion Program.

b. EO 13526, Classified National Security Information (NSI).

c. EO 13556, Controlled Unclassified Information (CUI).

d. EO 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information.

e. EO 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.

f. EO 13833, Enhancing the Effectiveness of Agency Chief Information Officers (CIOs).

g. EO 14028, Improving the Nation’s Cybersecurity.

h. Homeland Security Presidential Directive (HSPD)-12, Policies for a Common Identification Standard for Federal Employees and Contractors, dated 8-27-2004.

i. National Cyber Strategy, dated 3-2-2023.

j. National Security Memorandum (NSM)-8, Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems.

k. National Security Presidential Memorandum (NSPM)-33, National Security Strategy for United States Government Research and Development.

l. Annual OMB Memorandum on FISMA Implementation.

m. Office of Management and Budget (OMB) Circular No. A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*.

n. OMB Circular No. A-130, *Managing Information as a Strategic Resource*.

o. OMB M 15-13, *Policy to Require Secure Connections Across Federal Websites and Web Services*.

p. OMB M 15-14, *Management and Oversight of Federal Information Technology*.

q. OMB M 17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*.

r. OMB M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*.

s. OMB M 19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*.

t. OMB M 19-26, *Update to the Trust Internet Connections (TIC) Initiative*.

u. OMB M 20-04, *Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements*.

v. OMB M-20-32, *Improving Vulnerability Identification, Management, and Remediation*.

w. OMB M 21-07, *Completing the Transition to Internet Protocol Version 6 (IPv6)*.

x. OMB M-21-30, *Protecting Critical Software Through Enhanced Security Measures*.

y. OMB M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*.

z. OMB M-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response*.

aa. OMB M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*.

bb. OMB M 22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*.

cc. OMB M-23-02, *Mitigating to Post-Quantum Cryptography*.

dd. Office of Personnel Management (OPM) 2021 Guide to Telework and Remote Work in the Federal Government.

ee. Presidential Policy Directive (PPD) 21, Critical Infrastructure Security and Resilience, dated 2-12-2013.

ff. PPD 40, National Continuity Policy, dated 7-15-2016.

gg. PPD 41, Federal Government Coordination Architecture for Significant Cyber Incidents, dated 7-26-2016.

hh. US-CERT, Federal Incident Notification Guidelines, dated 4-1-2017.

3. DEPARTMENT OF HOMELAND SECURITY (DHS). DHS Binding Operational Directives (BOD).

a. DHS BOD 18-01, *Enhance Email and Web Security*.

b. DHS BOD 19-02, *Vulnerability Remediation Requirements for Internet-Accessible Systems*.

c. DHS BOD 20-01, *Develop and Publish a Vulnerability Disclosure Policy*.

d. DHS BOD 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities*.

e. DHS BOD 23-01, *Improving Asset Visibility and Vulnerability Detection on Federal Networks*.

f. DHS Cybersecurity and Infrastructure Security Agency (CISA) Emergency Directive (ED) 19-01*, Mitigate DNS Infrastructure Tampering.*

g. DHS CISA ED 20-02, *Mitigate Windows Vulnerabilities from January 2020 Patch Tuesday.*

h. DHS CISA ED *20-03, Mitigate Windows DNS Server Remote Code Execution Vulnerability from July 2020 Patch Tuesday.*

i. DHS CISA ED 20-04*, Mitigate Netlogon Elevation of Privilege Vulnerability from August 2020 Patch Tuesday.*

j. DHS CISA ED 21-01*, Mitigate SolarWinds Orion Code Compromise.*

k. DHS CISA ED 21-02*, Mitigate Microsoft Exchange On-Premises Product Vulnerabilities.*

l. DHS CISA ED 21-03*, Mitigate Pulse Connect Secure Product Vulnerabilities.*

m. DHS CISA ED 21-04*, Mitigate Windows Print Spooler Service Vulnerability.*

n. DHS CISA ED 22-02*, Mitigate Apache Log4j Vulnerability (Closed).*

o. DHS CISA ED 22-03*, Mitigate VMware Vulnerabilities.*

4. DOE ISSUANCES.

a. Cyber Council Charter.

b. DOE Cybersecurity Strategy & Implementation Plan.

c. DOE Data Governance Board (DGB) Charter.

d. DOE Information Resources Management (IRM) Strategic Plan.

e. DOE Strategic Plan.

f. Information Management Governance Board (IMGB) Charter.

g. Integrated Joint Cybersecurity Coordination Center (iJC3) Charter.

h. DOE Records Management Handbook.

5. DOE ORDERS AND GUIDELINES. Information Technology and Information Security related DOE Issuances located at https://www.directives.doe.gov/directives, and include the current version of:

a. DOE O 142.3, *Unclassified Foreign National Access Program*.

b. DOE O 150.1B, *Continuity Programs*.

c. DOE O 151.1, *Comprehensive Emergency Management System*.

d. DOE O 200.1A Chg 1 (MinChg), *Information Technology Management*.

e. DOE O 206.1, *Department of Energy Privacy Program*.

f. DOE O 206.2 Chg 1, *Identity, Credential, and Access Management (ICAM)*.

g. DOE O 226.1B, *Implementation of Department of Energy Oversight Policy*.

h. DOE O 227.1A Chg 1, *Independent Oversight Program*.

i. DOE O 243.1C, *Records Management Program*.

j. DOE O 251.1D, *Departmental Directives Program*.

k. DOE O 360.1D, *Federal Employee Training*.

l. DOE O 415.1 Chg 2, *Information Technology Project Management*.

m. DOE O 452.8, *Control of Nuclear Weapon Data*.

n. DOE O 470.3C Chg 1, *Design Basis Threat (DBT) Order*.

o. DOE O 470.4B Chg 3, *Safeguards and Security Program*.

p. DOE O 470.5, *Insider Threat Program*.

q. DOE O 470.6 Chg 1, *Technical Security Program*.

r. DOE O 471.1B, *Identification and Protection of Unclassified Controlled Nuclear Information*.

s. DOE O 471.6 Chg 3, *Information Security*.

t. DOE O 471.7, *Controlled Unclassified Information*.

u. DOE O 472.2A, *Personnel Security*.

v. DOE O 475.2B, *Identifying Classified Information*.

w. DOE G 580.1A, DOE *Personal Property Management Program*.

6. COMMITTEE ON NATIONAL SECURITY SYSTEMS (CNSS). CNSS Policies, Directives, Instructions, and Issuances located at https://www.cnss.gov/CNSS/ and includes:

a. CNSS Instruction 1253, Security Categorization and Control Selection for National Security Systems.

b. CNSS Instruction 4004.1, Destruction and Emergency Protection Procedures for COMSEC and Classified Material.

c. CNSS Instruction 4009, Information Assurance Glossary.

d. CNSS Policy 22, Cybersecurity Risk Management Policy.

e. CNSS Policy 26, National Policy on Reducing the Risk of Removable Media for National Security Systems.

7. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). NIST Standards, Frameworks, Special Publications for Information Security are located at https://csrc.nist.gov/Publications.

a. NIST Standards and Frameworks Include:

(1) NIST Federal Information Processing Standards Publication (FIPS) 140-3, Security Requirements for Cryptographic Modules.

(2) NIST FIPS 199, Standards for Security Categorization of Federal Information and Information Systems.

(3) NIST FIPS 200, Minimum Security Requirements for Federal Information and Information Systems.

(4) NIST FIPS 201, Personal Identity Verification of Federal Employees and Contractors.

(5) NIST Framework for Improving Critical Infrastructure Cybersecurity v1.1.

(6) NIST Interagency Report (IR) 7298 Revision 1, Glossary of Key Information Security.

b. NIST Special Publication (SP) 800 series (not all-inclusive) – current version:

(1) NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems.

(2) NIST SP 800-30, Guide for Conducting Risk Assessments.

(3) NIST SP 800-34, Contingency Planning Guide for Federal Information Systems.

(4) NIST SP 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.

(5) NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View.

(6) NIST SP 800-46, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security.

(7) NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations.

(8) NIST SP 800-53A, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans.

(9) NIST SP 800-59, Guideline for Identifying an Information System as a National Security System.

(10) NIST SP 800-60, Volume 1, Guide for Mapping Types of Information, and Information Systems to Security Categories.

(11) NIST SP 800-60, Volume 2, Guide for Mapping Types of Information, and Information Systems to Security Categories: Appendices.

(12) NIST SP 800-61, Computer Security Incident Handling Guide.

(13) NIST SP 800-63, Digital Identity Guidelines.

(14) NIST SP 800-82, Guide to Operational Technology (OT) Security.

(15) NIST SP 800-88, Guidelines for Media Sanitization.

(16) NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems.

(17) NIST SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations.

(18) NIST SP 800-150, Guide to Cyber Threat Information Sharing.

(19) NIST SP 800-160, Volume 1, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems.

(20) NIST SP 800-161, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.

(21) NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.

(22) NIST SP 800-181, NIST National Initiative for Cybersecurity Education (NICE).

(23) NIST SP 800-207, Zero Trust Architecture.

(24) NIST SP 800-213, NISTIRs 8259A/B/C/D: Guidance Draft for Federal Agencies and IoT Device Manufacturers.

ATTACHMENT 6
DEFINITIONS AND ACRONYMS

This Attachment provides information associated with DOE O 205.1D as well as information applicable to contracts in which the associated CRD (Attachment 1 to DOE O 205.1D) is inserted.

DEFINITIONS

Refer to *NIST Interagency Report (IR) 7298 Revision 1, Glossary of Key Information Security Terms* for additional definition related to cybersecurity, but not unique to this Order. The NIST IR 7298 Rev 1 includes most of the current terms & definitions used in NIST information security publications and those in the Committee on National Security Systems (*CNSS) Instruction No. 4009, National Information Assurance (IA) Glossary*. Additional DOE terms are provided in Table 6-1 below.

Table 6-1 Definitions

#	Term	Definition
1	Assessment and Authorization (A&A)	The official management decision given by a senior Federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls inherited by agency information systems.
2	Assurance System	Encompasses all aspects of the processes and activities designed to identify deficiencies and opportunities for improvement, report deficiencies to the responsible managers, complete corrective actions, and share in lessons learned effectively across all aspects of operation. Often referred to as Contractor Assurance System (CAS) for an M&O organization.
3	Controlled Unclassified Information (CUI)	Controlled Unclassified Information (CUI) is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. CUI does not include classified or information a non-executive

#	Term	Definition
		branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency.
4	Critical Software	Any software that has, or has direct software dependencies upon, one or more components with at least one of these attributes: • Is designed to run with elevated privilege or manage privileges; • Has direct or privileged access to networking or computing resources; • Is designed to control access to data or operational technology; performs a function critical to trust; or, • Operates outside of normal trust boundaries with privileged access.
5	Cybersecurity	The physical, technical, and administrative controls and risk management processes for providing the required and appropriate level of confidentiality, integrity, availability, and accountability for DOE/NNSA information stored, processed, or transmitted on electronic systems (and networks).
6	Data	Data includes all structured and unstructured files and fragments that reside or have resided in federal systems, devices, networks, applications, databases, infrastructure, and backups (including on-premises and virtual environments) as well as the associated metadata.
7	DOE Federal System	Includes systems operated by the DOE or by contractors on behalf of the DOE where the system is used to accomplish a Federal function. Does not include systems operated by M&O contractors unless such systems meet the above definition.
8	DOE Oversight	Encompasses activities performed by DOE organizations to determine whether Federal and contractor programs and management systems, including assurance and oversight systems, are performing effectively and/or complying with DOE requirements. Oversight programs include operational awareness activities, onsite reviews, assessments, self-assessments,

#	Term	Definition
		performance evaluations, and other activities that involve evaluation of contractor organizations and Federal organizations that manage or operate DOE sites, facilities, or operations.
9	Federal Record	Includes all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them; and does not include: • Library and museum material made or acquired and preserved solely for reference or exhibition purposes; or • Duplicate copies of records preserved only for convenience.
10	Government-Furnished Equipment	Includes, but is not limited to, laptop computers, mobile phones, mobile Wi-Fi hotspots (MiFi), memory cards, external drives, thumb drives, and other mobile computing/storage devices purchased by or on behalf of DOE.
11	Heads of Departmental Elements (HDEs)	Per DOE O 251.1D, *Departmental Directives Program*, include the Assistant Secretaries and Program Office Directors reporting to the Secretary either directly or through the Deputy Secretary or Under Secretaries. The NNSA Administrator is the only NNSA HDE. Power Marketing Administrators are HDEs.
12	Integrated Joint Cybersecurity Coordination Center (iJC3)	Managed and operated by DOE CIO. iJC3 provides incident response, reporting, tracking, and other computer security support to collect, analyze, and share cybersecurity information and to serve as the incident response coordination and reporting element across the Enterprise [DOE HQ; NNSA; Office of Environmental Management, Office of Legacy Management, Office of Energy; Office of Science; Energy Information Administration, Power Marking Administrations (PMA); laboratories, plants, and sites] and the energy sector.

#	Term	Definition
13	INFOCON	The INFOCON system presents a structured, coordinated approach to defend against and react to adversarial attacks on DOE information, computer systems, and telecommunication networks and systems.
14	Information Assurance Response Center (IARC)	NNSA's Information Assurance Response Center (IARC) continuously monitors all activity going through the nuclear security enterprise computer firewall system, providing intrusion detection and event forensics for the NNSA enterprise.
15	Limited Area	A type of security area having boundaries defined by physical barriers, used for the protection of classified matter and/or Category III quantities of special nuclear material, where protective personnel or other internal controls can prevent access by unauthorized people to classified matter or special nuclear material.
16	Major Incident	A major incident is: 1. Any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people. DOE should determine the level of impact of the incident by using the existing incident management process established in The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61, *Computer Security Incident Handling Guide*; or 2. A breach that involves PII that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people.
17	Multi-Factor Authentication	Authentication using two or more factors to achieve authentication. Factors include: • Something you know (e.g., password/personal identification number [PIN]); • Something you have (e.g., cryptographic identification device, token); or

#	Term	Definition
		• Something you are (e.g., biometric)
18	National Manager	The National Manager is the Director of the National Security Agency.
19	National Security Systems	A National Security System (NSS) is any information system (including any telecommunications system) that is used or operated by an agency, a contractor of an agency, or another organization on behalf of an agency where the use or operation involves intelligence activities, cryptologic activities related to national security, command and control of military forces, or is an integral part of a weapon or weapons system. This also encompasses systems used to support military or intelligence missions. Systems that are specifically identified within approved legislation or executive order and must be kept classified in the interest of national defense or foreign policy are also considered NSS. All U.S. Government classified networks have also been designated as NSS.
20	Operational Technology	Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes, and events in the enterprise.
21	POA&M	The authoritative agency management tool for managing system risk and are used in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in agency programs and systems.
22	Personally Identifiable Information (PII)	Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.
23	Portable Electronic Device	These devices have the capability to store, record, and/or transmit text, images/video, or audio data from one system to another. Examples of such devices include, but are not limited to: pagers, laptops, cellular telephones, radios, compact disc and

#	Term	Definition
		cassette players/recorders, portable digital assistant, audio devices, watches with input capability, and reminder recorders. Portable devices can also include those devices which would allow the transfer of DOE data either externally or internally such as removable memory-based media and removable devices that incorporate storage (e.g., Phones, iPod, etc.).
24	Protected Area	A type of security area defined by physical barriers (i.e., walls or fences) and surrounded by intrusion detection and assessment systems, to which access is controlled, used to protect Category II special nuclear material and classified matter and/or to provide a concentric security zone surrounding a material access area or a vital area.
25	Recorded Information	Includes all traditional forms of records, regardless of physical form or characteristics, including information created, manipulated, communicated, or stored in digital or electronic form.
26	Technical Surveillance Countermeasures (TSCM)	TSCMs are the techniques and measures used to detect, isolate, and nullify the technologies that are intended to obtain unauthorized access to classified and/or unclassified controlled information.
27	Unclassified Controlled Technical Information (UCTI)	Technical data or computer software (as defined in Defense Federal Acquisition Regulation Supplement 252.227-7013) with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.
28	Virtual Private Networks (VPN)	A virtual private network (VPN) is a mechanism for creating a secure connection between a computing device and a computer network, or between two networks, using an insecure communication medium such as the public Internet.
29	Zero Trust Architecture	A security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The zero-trust security

#	Term	Definition
		model eliminates implicit trust in any one element, component, node, or service and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses.

ACRONYMS

Acronyms used in this Order are listed in Table 6-2 below.

Table 6-2 Acronyms

Acronym	Abbreviated Term
A&A	Assessment and Authorization
AAL	Authenticator Assurance Level
AO	Authorizing Official
AODR	Authorizing Official Designated Representative
ATO	Authorization to Operate
AV	Antivirus
BOD	Binding Operational Directive
BYOD	Bring Your Own Device
CDM	Continuous Diagnostics and Mitigation
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer

Acronym	Abbreviated Term
CO	Contracting Officer
COMSEC	Communication Security
COOP	Continuity of Operations
COR	Central Office of Record
CRD	Contractor Requirements Document
CNSS	Committee on National Security Systems
CSF	Cybersecurity Framework
CSP	Cloud Service Provider
CSPP	Cybersecurity Program Plan
C-SCRM	Cyber Supply Chain Risk Management
CUI	Controlled Unclassified Information
DE	Departmental Element
DE-CSPP	Departmental Element Cybersecurity Program Plan
DHS	Department of Homeland Security
DLP	Data Loss Prevention
DNS	Domain Name Service
DOE	Department of Energy
EA	Enterprise Assessments

Acronym	Abbreviated Term
E-CSPP	Enterprise Cybersecurity Program Plan
eCC	Electronic Country Clearance
EDs	Emergency Directives
EDR	Endpoint Detection and Response
EGRC	Enterprise Governance, Risk Management and Compliance
FAL	Federation Assurance Level
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
FRD	Formerly Restricted Data
GAO	Government Accountability Office
GC	Office of the General Counsel
GFE	Government-Furnished Equipment
GSA	U.S. General Services Administration
HDE	Heads of Departmental Element
HVA	High Value Asset
IAL	Identity Assurance Level
IARC	Information Assurance Response Center
iJC3	Integrated Joint Cybersecurity Coordination Center

Acronym	Abbreviated Term
INFOCON	Information Operations Condition
IOT	Internet of Things
IP	Intellectual Property
IT	Information technology
LA	Limited Area
LOA	Level of assurance
MAA	Material Access Area
MFA	Multi-factor Authentication
M&O	Management and Operating
NARA	National Archives and Records Administration
NERC	North American Electric Reliability Corporation
NIST	National Institute for Standards and Technology
NNSA	National Nuclear Security Administration
NSS	National Security Systems
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
OT	Operational Technology

Acronym	Abbreviated Term
PA	Protected Area
P.L.	Public Law
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PMA	Power Marketing Administration
PNA	Privacy Needs Assessment
POA&M	Plan of Action and Milestones
RD	Restricted Data
SAISO	Senior Agency Information Security Officer
SAOP	Senior Agency Official for Privacy
SCRM	Supply Chain Risk Management
SDLC	System Development Lifecycle
SOP	Standard Operating Procedure
SP	Special Publication
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
TFNI	Trans-classified Foreign Nuclear Information

Acronym	Abbreviated Term
TSCM	Technical Surveillance Countermeasure
UERM	Universal Electronic Records Management
UCNI	Unclassified Controlled Nuclear Information
UCTI	Unclassified Controlled Technical Information
US-CERT	United States Computer Emergency Readiness Team
VDP	Vulnerability Disclosure Program
VPN	Virtual Private Network
ZTA	Zero Trust Architecture