U.S. Department of Energy
Washington, DC

ORDER

DOE O 205.1C

Approved: 5-15-2019
Chg 1 (LtdChg): 2-3-2022

SUBJECT: DEPARTMENT OF ENERGY CYBERSECURITY PROGRAM

1. PURPOSE. Enable accomplishment of the Department's mission and fulfill Federal cybersecurity requirements while allowing Departmental Elements (DEs) programmatic and operational flexibility, enhancing risk management, enabling effective implementation, delegating risk management to the lowest appropriate level, addressing roles and responsibilities, and setting standards for performance across all levels of the Department.

2. CANCELLATION. DOE O 205.1C, *Department of Energy Cybersecurity Program*, dated 05-15-2019. 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contract unless and until the contract or regulatory commitment is modified to either eliminate requirements that are no longer applicable or substitute a new set of requirements.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.

      (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 Bonneville Power Administration will assure that its employees and contractors comply with their respective responsibilities under this directive.

   b. Department of Energy (DOE) Contractors. Except for the equivalencies/ exemptions in paragraph 3.c., the CRD, Attachment 1, sets forth requirements of this Order, including those requirements contained in Attachment 2, that will apply to certain Management and Operating (M&O) contracts and non-M&O Major Site/Facility contracts as determined by the Heads of Departmental Elements (HDEs).

      (1) The M&O and non-M&O Major Site/Facility contracts that must include the CRD are those at sites and facilities that collect, create, process, transmit, store, or disseminate data on information systems and operational technology for DOE or on the behalf of DOE.

(2) The CRD also forms the basis for equivalent requirements, that may be included in contract clauses or other contract provisions, applicable to non-M&O, Major Site/Facility contracts that collect, create, process, transmit, store, or disseminate data on information systems.

c. Equivalencies/Exemptions for DOE O 205.1C.

(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) Exemption. None.

4. REQUIREMENTS. The DOE Cybersecurity Program is a shared, distributed enterprise risk management approach to protect DOE information systems to comply with the Federal Information Security Modernization Act of 2014 (FISMA) and in alignment with the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) of NIST Special Publication (SP) 800-37 and NIST Framework for Improving Critical Infrastructure Cybersecurity – abbreviated as Cybersecurity Framework (CSF). Additionally, the DOE Cybersecurity Program protects its National Security Systems (NSSs) to comply with the requirements of Committee for NSS (CNSS) issuances. The DOE Cybersecurity Program approaches implementation of cybersecurity requirements in a manner commensurate with impact to mission, national security, risk, and magnitude of harm, as well as addressing both information technology (IT) and operational technology systems. The DOE Cybersecurity Program empowers HDEs and provides them the flexibility to tailor and implement cybersecurity risk mitigation controls in consideration of threats, acceptable risks, mission needs, and environmental, and operational factors. Risk management is also to be performed in accordance with other DOE Directives, as applicable.

a. To implement the DOE Cybersecurity Program, the Department maintains:

(1) An 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 the HDEs. The E-CSPP addresses the RMF steps and CSF from the Department's overall organizational perspective.

(2) CSPPs, which are required for all DOE DEs and their associated sites that manage IT/OT systems. DE-CSPPs and Site CSPPs must cover all DOE systems and all DOE IT assets. Consolidated, combined or subordinate CSPPs may be used as needed to address organizational structures, shared service arrangements, and mission requirements. DE-CSPPs address the

CSF alignment and the RMF steps from their organizational, mission/business and system perspectives. Sites abide by DE-CSPP through contracting processes described in this order or by inheritance/adoption of DE-CSPP for Federal sites.

(3) In support of the preceding documents in paragraphs 3.a.(1) and (2), DOE Office of the CIO (OCIO) issues non-binding amplifying cybersecurity guidance, which may be adopted or tailored to individual DE/Site needs to meet requirements. The OCIO issuances equip DE/Sites with cost effective options for meeting Federal compliance and facilitate inheritance of enterprise solutions for their DE-CSPPs.

Note: The NNSA maintains a Supplemental Directive to provide additional requirements and amplifying guidance on implementation of the DOE Cybersecurity Program for its component activities.

b. Communication Security (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).

c. 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 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.

(1) For National Security Systems (NSS) protections, DEs/Sites must comply with the requirements of Committee for NSS (CNSS). DEs/Sites must use NIST SP 800-59, Guideline for Identifying an Information System, as a National Security System as guidance.

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

(3) For High Value Assets (HVAs), DEs must identify, report, and manage HVAs in accordance with Office of Management and Budget (OMB) Memorandum M-19-03, Strengthening the Cybersecurity of Federal

Agencies, by enhancing the HVA Program, in coordination with the DOE CIO.

(4) For Controlled Unclassified Information (CUI), Official Use Only (OUO), and Unclassified Controlled Technical Information (UCTI) on Non-Federal systems, DEs/Sites must adhere to the security requirements specified in NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations. Information that may be categorized as "CUI Specified" in accordance with the requirement of 32 CFR 2002 may have additional protection requirements specified under law, regulation, or Government-wide policies (LRGWP). Where the LRGWP does not address security requirements, the security requirements specified in NIST SP 800-171 apply.

d. The DOE OCIO will establish and maintain a DOE Cybersecurity Data Repository for key cybersecurity information described in paragraphs 3.b.(1)-(3). The Data Repository facilitates enterprise visibility and bi-directional information flows on key items for effective cybersecurity operations while maintaining empowered HDEs and DE/Site CISOs to manage their DE/Site-CSPPs. DEs/Sites in coordination with OCIO will update the repository with the appropriate frequency.

(1) Inventories.

(a) FISMA Systems and status. Name of FISMA System, applicable identification for enhanced controls including those in paragraph 4.b. and Authorizing Official (AO) contact information.

(b) Internet-facing Internet Protocol addresses and websites.

(2) Cybersecurity Posture.

(a) DE/Site Plan of Action and Milestones (POA&Ms) for:

1 HVAs - Monthly updates for any open items.

2 POA&Ms that cannot be closed in less than 30 days or require significant resources to close.

3 POA&Ms for Oversight Audits and Assessments including DOE Enterprise Assessments (EA), Government Accountability Office (GAO) and Office of Inspector General (OIG). Quarterly updates should be provided for any open items.

Note: POA&Ms other than the above are deferred to the DEs/Sites.

(b) DE/Site Cybersecurity Risk Register (Quarterly Updates).

(c) DE/Site Current and Target NIST CSF Profiles (Annual Updates).

(3) Names and Contact Information.

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

(b) DE/Site CIO, CISO, or individuals performing similar functions.

(c) DE/Site AOs.

(d) DE/Site designated representatives for routine cybersecurity data collection and reporting.

e. Common CSPP Topics. The E-CSPP and DE/Site-CSPPs must address requirements for the following items in accordance with the Federal laws, regulation, directives, policies, standards, and guides pertaining to cybersecurity, as well as interrelated DOE issuances, directives, policies, and procedures identified in Attachment 3:

(1) Scope and applicability.

(2) At least annual review and update of the CSPP.

(3) Cybersecurity roles, responsibilities, and authorities.

(4) Organization-defined cybersecurity policies, procedures and controls and control inheritance structures/processes.

(5) System inventory and identification of enhanced control types including HVAs, Personally Identifiable Information (PII), and other CUI-specified information types as identified in 32 CFR 2002.

(6) POA&M Process.

(7) Measures of performance.

(8) Exception and exemption processes for information security controls.

(9) Cybersecurity risk management strategy and approach for periodic risk assessments and management of risk registers with at least quarterly review and update.

(10) Information System Security plan processes.

(a) Unclassified systems including CUI, OUO, or other categories.

(b) Classified systems (if applicable).

(11) Authorization Process.

(a) Authorizing and managing systems.

(b) Authorizing and managing mobile devices.

(c) Authorizing and managing foreign national access to systems (if applicable).

(12) Cloud computing and use of Federal Risk and Authorization Management Program (FedRAMP) processes and tools, as applicable.

(13) Rules of behavior.

(a) Unprivileged users.

(b) Privileged users.

(c) Remote access and telework security.

(14) Threat Awareness Program and Automated Indicator Sharing (AIS).

(15) Incident handling and reporting.

(16) Cybersecurity testing and monitoring activities.

(17) Contingency Planning.

(18) Workforce and Training.

(a) General unprivileged and privileged user initial and refresher training.

(b) Cybersecurity workforce forums for sharing recommended practices and lessons learned.

(c) Authorizing Official (AO) responsibilities, delegations, qualifications, and reciprocity agreements.

(d) Cybersecurity role-based training requirements.

(e) Coordination of CIO, CISO, and AO roles.

(19) Information and Communications Technology Supply Chain Risk Management (SCRM).

(20) A current profile and target profile for cybersecurity per the NIST CSF.

f. E-CSPP. In addition to addressing the required common CSPP topics, the DOE CISO must implement and maintain an E-CSPP that addresses the following items from a Department-wide perspective:

(1) Enterprise Risk Management of Cybersecurity.

(a) Ensuring implementation of policies to reduce the level of risk.

(b) Support for making informed enterprise-level cybersecurity risk decisions.

(c) Processes to manage organization-wide cybersecurity risk assessment that include aggregation of system-level risk assessments.

(d) Incorporates qualitative and quantitative approaches to mature into the latest industry risk approaches.

(2) System Inventory. Ensuring DE/Site inventory of IT assets is managed for completeness and accuracy based on DOE Cybersecurity Data Repository.

(3) Measures of Performance.

(a) Processes for collecting, reporting cybersecurity data and metrics required by Federal law, regulation, or policy.

(b) Establishing key cybersecurity performance metrics that define and measure mission outcomes.

(4) Incident Handling and Reporting.

(a) Maintain Operation of the Department's integrated Joint Cybersecurity Coordination Center (iJC3) to ensure that the Department meets Federal Agency incident reporting requirements from OMB and the Department of Homeland Security.

(b) iJC3 operations must comply with classified information and incident handling procedures in Department Directives, including DOE O 470.4, *Safeguards and Security Program*, current version.

(c) iJC3 operations must comply with review requirements for documents that potentially contain classified information or Unclassified Controlled Nuclear Information (UCNI) under DOE O 475.2, *Identifying Classified information*, current version; and Title 10 Code of Federal Regulations (CFR), Part 1017,

Identification and Protection of Unclassified Controlled Nuclear Information.

(d) iJC3 establishes and maintains Standard Operating Procedures (SOPs) that align with United States Computer Emergency Readiness Team (US-CERT) Federal Incident Notification Guidelines and NIST SP 800-61, Computer Security Incident Handling Guide.

(e) Annual Department-wide cybersecurity incident response exercise.

(5) Cybersecurity Testing and Monitoring. Testing is conducted to ensure that controls are effectively implemented.

(6) Workforce and Training.

(a) Initial and periodic cybersecurity awareness refresher training is completed for general unprivileged and privileged users.

(b) Minimum Standards are established and maintained for AO and other priority cybersecurity role qualifications and a curriculum is developed and maintained that addresses initial and refresher training and continuing professional development.

(7) Threat Assessment. Joint management of the DOE enterprise cybersecurity threat assessment with IN in coordination with DEs. Technical Threat assessments must include input from AU and NNSA per CNSS and other policies for threat to information systems from technical means such as technical surveillance countermeasures (TSCM) and TEMPEST.

(8) Vulnerability Disclosure Program. Attachment 2 sets forth requirements and handling procedures for the Department's Vulnerability Disclosure Program in alignment with 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*.

(a) Implement a Vulnerability Disclosure Program (VDP) 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.

(b) Establish triage and assessment processes for reported vulnerabilities by external third parties.

(c) Maintain communication with external third parties on reported vulnerabilities.

(d) Track reported vulnerabilities in alignment with risk management and incident reporting metrics and processes.

(9) Bidirectional Reporting, Communications, and Collaboration.

(a) DOE cybersecurity dashboard and periodic reporting for leadership, management, cybersecurity professionals, and information resource management operators.

(b) Periodic status reporting to governing bodies.

(c) Formal processes to share lessons learned with DEs to increase situational awareness and improve DOE's collective cybersecurity posture.

(d) Processes, platforms and tools for sharing of cybersecurity threat data within the Department and with relevant Federal Agencies.

(10) Processes to leverage the Federal Risk and Authorization Management Program (FedRAMP).

(11) Maintain a DHS Rule of Engagement Authorization for HVAs and maintain support processes for HVA Assessments by DHS.

g. Coordination of the DOE Technical Security Program (TSP) from DOE O 470.6, *Technical Security Program*, current version, and the DOE Cybersecurity Program as well as processes to address any deviation from associated federal requirements are handled in accordance with governing directives.

h. Coordination for deviations involving COMSEC requirements must come from the DOE COMSEC COR to the appropriate National Authority.

i. DE-CSPP. In the addition to addressing the required common CSPP items, DEs must develop and maintain DE-CSPPs that address the following:

(1) Risk Management.

(a) Must provide the framework for establishing acceptable risk in context of mission performance and assurance, and in accordance with other DOE Directives, as applicable.

(b) For contractors, the Federal Oversight must provide a methodology and model 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 Owner in establishing acceptable risks.

(2) Authorization Process.

(a) Must address management of common controls for any systems that fall under its purview.

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

(c) Must accept risk, in writing, for residual risk if TEMPEST countermeasures requirements from Certified TEMPEST Technical Authority (CTTA) in accordance with CNSS issuance, by the appropriate program AO.

(3) Measures of Performance.

(a) Must 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*, current version, and related contract terms and conditions.

(b) Must establish processes for POA&M tracking and reporting cybersecurity weaknesses identified for information systems that integrate with continuous monitoring and risk management processes.

(4) Incident Handling and Reporting.

(a) Must define a process for incident reporting that requires 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 iJC3 in accordance with iJC3 procedures and guidance.

(b) 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, current version.

(c) Must include participation in annual Department-wide cybersecurity incident response exercises.

(d) Must include reporting incidents involving COMSEC materials and Controlled Cryptographic Items (CCI) to the DOE COR and handled at the direction of the COR.

(5) Workforce.

(a) Must ensure minimum standards are maintained for AO qualifications, and periodic refresher training, and continuing professional development.

(b) Should support enterprise collaboration for AOs to exchange best practices and lessons learned.

(c) 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.

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

(6) Classified Information Systems.

(a) 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.

(b) Must include requirements for identifying and protecting Restricted Data (RD), Formerly Restricted Data (FRD) and Trans-classified Foreign Nuclear Information (TFNI) on NSS consistent with DOE O 471.6, *Information Security*, current version;

DOE O 475.2, *Identifying Classified Information*, current version; and DOE O 452.8, *Control of Nuclear Weapon Data*, current version. When RD, FRD, or TFNI is provided to personnel from other Government Agencies, the CSPPs must ensure that such personnel follow the requirements contained in this Order.

(7) Contingency Planning. Must align contingency planning and continuity of operations (COOP) planning with DOE O 150.1, *Continuity Programs*, current version, to ensure restoring IT services in accordance with Business Impact Analysis (BIA) of systems to include consideration of those providing or supporting Mission Essential Functions.

(8) Warning Banner. Must require DOE and NNSA NSS and Federal unclassified systems to 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) A definition of information system that includes the computer, the DOE computer network, and all devices, such as storage media, connected to the computer;

(c) 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;

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

(e) The user acknowledges and 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, the Inspector General, or as mandated by law.

(f) 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, criminal penalties, and or financial liability for the cost of such improper use;

(g) 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 consistent with DOE O 203.1, *Limited Personal Use of Government Office Equipment including Information Technology*, current version, and any other applicable DOE Order or directive regarding use of DOE information systems;

2 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.

To the extent the usage banners satisfy the above provisions, such banners will be in compliance with DOE O 470.5, *Insider Threat Program*, dated 6-2-14. paragraph 4.f.

(9) Media Controls.

(a) Must address risk-based protection of information on media used by or produced by information systems using the NIST SP 800-53 controls.

(b) Must require appropriate media sanitization procedures.

(c) Must require disposal of electronic media in accordance with DOE and NNSA record retention schedules and requirements.

j. Existing System Authorizations and CSPPs.

(1) 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). Reauthorization must be in accordance with the applicable DE-CSPP and should incorporate continuous monitoring and ongoing authorization, where practical. Existing ongoing authorizations must be reevaluated in accordance with the applicable DE-CSPP. For contractors to fully assess the CRD the DE-CSPPs should be in place prior to requesting an assessment of effects.

(2) Existing CSPPs must be updated to address revised requirements of this Order within one year of its issuance.

k. Requirements for contractors are provided in the CRD as Attachment 1.

l. Requirements for COs when including the CRD in contracts. The HDE, or his or her designee, shall notify the CO and other appropriate subject matter experts in the organization that the directive applies to an existing contract or to a solicitation for a future contract. For existing contracts, the HDE shall designate appropriate representatives to work with the CO to develop an appropriately tailored set of standards, practices, and controls.

(1) For existing Management & Operating M&O contracts, after being notified by the HDE, or his or her designee, the CO shall provide the contractor the opportunity to assess the effect of incorporating the CRD on contract cost, funding, schedule, and technical performance, and to provide input on the appropriately tailored set of requirements for the contract. All associated activities will be accomplished in a timely manner and, if applicable, in accordance with the timelines established in Department of Energy Acquisition Regulation 970.5204-2. The CO will incorporate the CRD without alteration unless the directive permits alteration and the appropriate process is followed.

(2) For existing non-M&O contracts, after being notified by the HDE, or his or her designee, the CO shall attempt to incorporate the CRD bilaterally. If attempts to negotiate the CRD into the contract bilaterally are not successful, the CO shall consult with the Head of Contracting Activity, Headquarters program office, and General Counsel. The CO shall incorporate the CRD without alteration unless the CRD or directive permits alteration and the appropriate process is followed.

5. RESPONSIBILITIES.

a. Deputy Secretary (S2).

(1) Serves as the Secretary's (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) Is responsible and 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. 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, and the information systems used

or operated by DOE or by a DOE contractor or other organization on behalf of DOE.

(3) Establishes cybersecurity accountability and provides active support and oversight of monitoring and improvement for the DOE Cybersecurity Program. Cybersecurity Program activities are orchestrated with the Privacy Program, which is defined in DOE Order 206.1, *Privacy Program*, current version.

(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.

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

(6) Issues—in consultation with the DOE CIO—Department-wide cybersecurity threat statements where timely remedial measures to protect against newly defined risks may be needed to protect DOE IT asset, information systems, or information from harm. AOs are then responsible for ensuring that appropriate actions are taken.

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

c. Heads of Departmental Elements (HDEs).

(1) Have overall responsibility for the DE-CSPP in accordance with paragraph 4 requirements within their DEs, 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.

(2) Use a risk-based and tailored approach to flow down the requirements and responsibilities of this Order to all subordinate organizational levels through 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) Designate AOs and define any further delegation within the DE. Also ensure that standards are maintained for AO qualifications, initial and refresher training, and continuing professional development.

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

(7) Participate in development of the Department's Cybersecurity Risk Management Strategy and then lead its implementation for their DE/Site in alignment with the System Development Lifecycle (SDLC) from NIST SP 800-64, Security Considerations in the SDLC.

(8) 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.

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

(10) Use bi-directional communication and reporting information flows to ensure that risk is addressed throughout the organization.

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

(12) Determine which M&O and non-M&O Major Site/Facility contracts must include the CRD and notify COs to incorporate the CRD. Determine which non-M&O, non-M&O Major Site/Facility Advisory and Assistance contracts must include equivalent requirements to the CRD (in a contract clause or other contract provision, for example, in the Statement of Work), and notify COs to include the equivalent requirements in the contracts.

(13) Establish written procedures within their organizations with clear lines of accountability that identify the organizational element responsible for identifying cybersecurity contract requirements, including applicability of the CRD, and for notifying the CO on which contracts must incorporate the CRD or equivalent contract requirements (for non-M&O Advisory and Assistance Service contracts).

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)/Chief Information Security Officer (CISO).

(b) Developing and maintaining the Department's Cybersecurity Program, along with associated cybersecurity policies, procedures, and control techniques to address information security requirements.

(c) Overseeing personnel with significant responsibilities for cybersecurity and ensuring that the personnel are adequately trained.

(d) Assisting HDEs with their cybersecurity responsibilities.

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

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

(a) An E-CSPP is effectively implemented, resulting in adequate cybersecurity for all organizational systems and environments of operation.

(b) Cybersecurity and SCRM considerations are integrated into programming, planning, budgeting cycles; enterprise architectures; the SDLC; and acquisitions.

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

(d) 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.

(e) 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.

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

(4) 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 and implements plans, procedures, and testing to ensure COOP for Department information systems.

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

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

(5) Under Federal Information Technology Acquisition Reform Act (FITARA) responsibilities, coordinates Department-wide IT and 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 investments, data center consolidation, IT training, and the review and approval of all Department IT and cybersecurity acquisition/procurement activities. Activities include leveraging Government Service Administration (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 National Initiative for Cybersecurity Education (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 Federal cybersecurity budget, to include any reprogramming of funds for these items.

(6) Serves as the Senior Agency Official for Privacy (SAOP). Oversees Departmental compliance with privacy law, regulations, OMB guidance and DOE O 206.1, current version.

(a) Serves as the principal organizational official authorized to accept privacy risk to organizational operations, assets, contracts, and individuals, as defined by OMB and NIST requirements.

(b) Ensures the protection of PII both at rest and in transit within, across, and external to DOE IT systems and networks.

(c) Oversees response to data breaches involving PII.

(d) Convenes and chairs the Department's Privacy Incident Response Team (PIRT).

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

(8) Coordinates with the TSP Director on the DOE cybersecurity matters that directly or indirectly affects the implementation of TSP including:

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

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

(c) Coordinating with DOE TSP to facilitate exchange of information specific to threats to information systems.

(d) Assisting with representation of the Department's cybersecurity position as it relates to TSP including official representation or

responses to Other Government Agencies (OGAs) on cybersecurity issues related to CIO authorities.

(e) Alerting the Director TSP 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.

(f) Providing support to activities for TSP required in the TSP Order.

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

e. DOE Chief Information Security Officer (CISO).

(1) Carries out the SAISO responsibilities required by Federal law, regulation, and policy. Works with DE/Site 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. The DOE CISO's organization supports the development and execution of the E-CSPP.

(3) Is designated by the CIO as the Enterprise AO. The DOE CISO maintains a register of the DOE's AOs and serves as the primary liaison for the CIO to the Department's AOs, system owners, and information system security officials.

(4) 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, the Office of Environment, Health, Safety and Security, Office of Cybersecurity Energy Security and Emergency Response, 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.

(d) Coordinating with the DOE CIO/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 and communications technology SCRM.

(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.

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. Chief Privacy Officer (CPO). Advises the SAOP on privacy matters. Coordinates with the DOE CISO to ensure coordination of privacy and information security and risk management activities related to the protection of PII.

(1) Supports the implementation of protections for PII in any format.

(2) Informs the SAOP and DOE CISO of potential risks to privacy involving information systems, and recommends steps to mitigate those privacy risks.

(3) Serves as the SAOP's authorized designee for privacy risk and compliance, as needed.

h. 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.

i. Authorizing Officials (AOs). The AO is a senior official or executive with the authority to formally assume responsibility and accountability for operating an

information system; providing common controls inherited by organizational systems; or using a system, service, or application from an external provider.

(1) Are the organizational officials who can accept the information security risk to organizational operations, organizational assets, and individuals.

(2) May provide hosting, operations, and/or technical support of the system; or in the case of M&O systems, are a Federal 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) Must be Federal officials who are responsible and accountable to their HDEs for ensuring that information systems under their purview are operated at an acceptable level of risk, which should be documented and communicated to the appropriate officials.

j. System Owners. Typically have budgetary oversight for the system or are responsible for the mission and/or business operations supported by the system.

k. Chief Acquisition Officer/Cognizant Senior Procurement Executive. Develops Departmental procurement policies and regulations, and issues procurement guidance to Contracting Officers. 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. Governance Bodies. Boards and Councils established by senior officials that advise the Department's senior decision makers. HDEs coordinate and collaborate on IT 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 Attachment 3.

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

(1) Serves as the AO for DOE information systems under the purview of 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. Associate Under Secretary for Environment, Health, Safety and Security (AU).

(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 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 3 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 AND ACRONYMS. Attachment 4 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

CONTRACTOR REQUIREMENTS DOCUMENT (CRD)
DOE O 205.1C, *DEPARTMENT OF ENERGY CYBERSECURITY 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.

In addition to the requirements set forth in this CRD, contractors are responsible for complying with Attachment 2 to DOE O 205.1C, referenced in and made a part of this CRD, which provides information and requirements applicable to contracts in which this CRD is inserted.

1. This CRD does not invoke any Technical Standards. Any Technical Standard mentioned or referenced in this CRD must not be considered to have been invoked. General Requirements. The Contractor Must:

    a. Assess and manage risk within its environment, in the context of acceptable mission risk set collaboratively with the Federal Site Manager.

    b. 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, and (2) approved oversight and assurance systems.

    c. Establish a Site Cybersecurity Program Plan (CSPP) that is consistent with the requirements of the applicable Departmental Element (DE) CSPP.

    d. Establish and maintain an effective *Assurance System* that provides appropriate transparency to Federal Oversight regarding cybersecurity risk management and overall performance.

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

    f. Establish a process to ensure that users acknowledge and consent to privacy and monitoring policies.

    g. Establish and maintain a process to support the Vulnerability Disclosure Program for vulnerabilities reported to in-scope DOE websites and systems.

    h. Establish and maintain an Incident Management Handling and Reporting Capability that is consistent with the contractor requirements contained within the applicable DE-CSPP.

    i. The contractor must ensure that security specifications are included in procurements of components for IT and OT.

2. National Security Systems (NSSs) Requirements. In addition to the general requirements, contractors with NSSs must:

   a. Adhere to the requirements established by the Committee on National Security Systems (CNSS). Requests for equivalencies and for exemptions from CNSS requirements must follow those processes, as amplified by direction within the applicable DE-CSPP.

   b. Ensure that security specifications are included in procurements of components for NSSs.

   c. Establish warranty clauses 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).

   d. Implement DOE classified data protection levels as defined in their respective DE-CSPPs or applicable to 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.

   e. Implement requirements for accessing, identifying and protecting Restricted Data (RD), Formerly Restricted Data (FRD) and Trans-classified Foreign Nuclear Information (TFNI) as defined in the DE-CSPPs.

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

This Attachment provides information and/or requirements associated with DOE O 205.1C as well as information and/or requirements applicable to contracts in which the associated CRD (Attachment 1 to DOE O 205.1C) 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, i.e., intended for use by the public or are internet-accessible through a publicly routed 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 2 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.[1]

[1] Definition of control adopted from NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.

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, 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 integrated Joint Cybersecurity Coordination Center (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)[2] during this process; and

(d) Reporters are encouraged to assess the potential impact of the vulnerability they are submitting via 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

[2] Further clarification on PII can be found in NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).

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.

(7) This Attachment will be effective upon the approval and issuance of DOE O 205.1C Chg 1. All Departmental Elements must be in compliance with this Attachment within one year of issuance.

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 has 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 and reported 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 Heads of Departmental Elements (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) Heads of Departmental Elements 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, the Federal Information Security Modernization Act (FISMA) of 2014, 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 CIO 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. DOE Order (O) 205.1C, *Department of Energy Cybersecurity Program*, enables accomplishment of the Department's mission and fulfills Federal cyber security requirements while allowing Departmental Elements programmatic and operational flexibility, enhances risk management, through delegation of risk management to the lowest appropriate level, addresses roles and responsibilities, and sets standards for performance across all levels of the Department.

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

h. 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:

> 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."[3]

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

[3] ISO / IEC 29147:2018, Information Technology – Security Techniques – Vulnerability Disclosure. §3.1.

ATTACHMENT 3. REFERENCES

This Attachment provides requirements associated with DOE O 205.1C.

1. FEDERAL LAWS AND REGULATIONS.

   a. Cybersecurity Act of 2015, Pub.L. No. 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.

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

   c. Title 44 United States Code (U.S.C.) 3542 Information Security Definitions.

   d. Title 32 Code of Federal Regulations (CFR) § 2001.23, Classification Marking in the Electronic Environment.

   e. Title 32 Code of Federal Regulations (CFR) § 2002, Controlled Unclassified Information (CUI).

   f. 10 CFR § 1045, Nuclear Classification and Declassification.

   g. 10 CFR § 1017, Identification and Protection of Unclassified Controlled Nuclear Information.

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

      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.

2. NATIONAL CYBERSECURITY POLICIES AND GUIDANCE.

   a. National Cyber Strategy, dated 9-20-2018.

   b. Executive Order (E.O.) 13526, Classified National Security Information (NSI), dated 12-29-2009.

   c. E.O. 13833, Enhancing the Effectiveness of Agency Chief Information Officers (CIOs), dated 5-15-2018.

d. Presidential Policy Directive (P.P.D) 41, Federal Government Coordination Architecture for Significant Cyber Incidents, dated 7-26-2016.

e. E.O. 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, dated 5-11-2017.

f. US-CERT,0 Federal Incident Notification Guidelines, dated 4-1-2017.

g. FedRAMP Memo, Security Authorization of Information Systems.

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

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

4. DOE ISSUANCES.

a. DOE Strategic Plan.

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

c. DOE Cybersecurity Strategy & Implementation Plan.

d. Information Management Governance Board (IMGB) Charter.

e. Cyber Council Charter.

f. iJC3 Charter.

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 150.1, *Continuity Programs*.

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

c. DOE O 203.2, *Mobile Technology Management*.

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

e. DOE O 206.2, *Identity, Credential, and Access Management (ICAM)*.

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

g. DOE O 227.1, *Independent Oversight Program*.

h. DOE O 243.1, *Records Management Program*.

i. DOE O 251.1, *Departmental Directives Program*.

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

k. DOE O 470.3, *Design Basis Threat (DBT) Order*.

l. DOE O 470.4, *Safeguards and Security Program*.

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

n. DOE O 470.6, *Technical Security Program*.

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

p. DOE O 471.6, *Information Security*.

q. DOE O 472.2, *Personnel Security*.

r. DOE O 473.3, *Protection Program Operations*.

s. DOE O 475.2, *Identifying Classified Information*.

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, 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 Framework for Improving Critical Infrastructure Cybersecurity.

(2) NIST Federal Information Processing Standards Publication (FIPS) 201, Personal Identity Verification of Federal Employees and Contractors.

(3) NIST FIPS 140-2, Security Requirements for Cryptographic Modules.

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

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

b. NIST Special Publications (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, Guide for Applying the Risk Management Framework to Information Systems: A Security Life Cycle Approach.

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

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

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

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

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

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

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

(12) NIST SP 800-64, Security Considerations in the System Development Life Cycle.

(13) NIST SP 800-82, Guide to Industrial Control System (ICS) Security.

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

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

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

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

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

(19) NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations.

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

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

ATTACHMENT 4. DEFINITIONS AND ACRONYMS

This Attachment provides information associated with DOE O 205.1C as well as information applicable to contracts in which the associated CRD (Attachment 1 to DOE O 205.1C) 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 4-1 below.

Table 4-1 Definitions

#	Term	Definition
1	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.
2	Controlled Unclassified Information (CUI)	Information that law, regulation or government-wide policy requires to have safeguarding or disseminating controls excluding information that is classified. Reference CUI Registry at www.archives.gov/cui.
3	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).
4	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.

#	Term	Definition
5	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, performance evaluations, and other activities that involve evaluation of contractor organizations and Federal organizations that manage or operate DOE sites, facilities, or operations.
8	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.
6	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.
7	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.

ACRONYMS

Acronyms used in this Order are listed in Table 4-2 below.

Table 4-2 Acronyms

Acronym	Abbreviated Term
AO	Authorizing Official
AODR	Authorizing Official Designated Representative
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CNSS	Committee on National Security Systems
CO	Contracting Officer
CRD	Contractor Requirements Document
CSF	Cybersecurity Framework
CSPP	Cybersecurity Program Plan
CUI	Controlled Unclassified Information

Acronym	Abbreviated Term
DE	Departmental Element
DE-CSPP	Departmental Element Cybersecurity Program Plan
DHS	Department of Homeland Security
DOE	Department of Energy
E-CSPP	Enterprise Cybersecurity Program Plan
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Protection Standard
FISMA	Federal Information Security Modernization Act
FRD	Formerly Restricted Data
HDE	Heads of Departmental Element
HVA	High Value Asset
iJC3	Integrated Joint Cybersecurity Coordination Center
IP	Intellectual Property
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
OMB	Office of Management and Budget
P.L.	Public Law
PII	Personally Identifiable Information
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
TFNI	Trans-classified Foreign Nuclear Information
UCTI	Unclassified Controlled Technical Information
US-CERT	United States Computer Emergency Readiness Team
VDP	Vulnerability Disclosure Program