SUPPLEMENTAL DIRECTIVE

NNSA SD 205.1

Approved: 7-6-17

BASELINE CYBERSECURITY PROGRAM

NATIONAL NUCLEAR SECURITY ADMINISTRATION
Office of Information Management and Chief Information Officer

CONTROLLED DOCUMENT
AVAILABLE ONLINE AT:
https://nnsa.energy.gov/aboutus/ouroperations/managementandbudget/supplementaldirectives
printed copies are uncontrolled

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

THIS PAGE INTENTIONALLY LEFT BLANK

BASELINE CYBERSECURITY PROGRAM

1. PURPOSE. This supplemental directive (SD) establishes an integrated, organization-wide Risk Management Approach (RMA) for the National Nuclear Security Administration (NNSA) to improve and maintain an agile Cybersecurity Program (CSP) in order to protect organizational operations and assets in a manner consistent with associated risks. This SD supplements the requirements of Department of Energy (DOE) Order 205.1B, *Department of Energy Cyber Security Program*. The SD also prescribes a CSP that employs a Risk Management Framework (RMF) that is:

   a. Based on the principles, responsibilities, processes, and oversight requirements in SD 226.1B, *NNSA Site Governance*; and

   b. Consistent with and incorporates National Institute of Standards and Technology (NIST), Committee on National Security Systems (CNSS), and DOE requirements and guidelines.

2. CANCELLATION.

   a. NAP-14.1D, *NNSA Baseline Cybersecurity Program*, dated 12-18-12.

   b. NAP 14.3B, *Transmission of Restricted Data over Secret Internet Protocol Router Network (SIPRNet)*, dated 5-02-08.

   c. Chapter VII, Incident Management of NAP-14.1C, *NNSA Baseline Cybersecurity Program.*

   Cancellation of a directive does not, by itself, modify or otherwise affect any contractual or regulatory obligation to comply with the directive's requirements. Cancelled directives that are incorporated by reference in a contract remain in effect until the contract is modified to delete the reference to the requirements in the cancelled directive.

3. APPLICABILITY.

   a. Federal. This SD applies to all NNSA federal entities that collect, create, process, transmit, store, and disseminate information on automated information systems (ISs) for NNSA.

   b. Contractors. Except for the equivalencies and exemptions in paragraph 3.c., the Contractor Requirements Document (CRD), Attachment A, sets forth requirements of this SD that will apply to site and facility management contracts.

      The CRD must be included in the management contracts for all sites and facilities that collect, create, process, transmit, store, and disseminate information on automated information systems for NNSA. Additionally, management contracts must include DOE Acquisition Regulation (DEAR) clause 952.204-77, *Computer Security*.

c. Equivalencies/Exemptions.

(1) Equivalency. In accordance with the responsibilities and authorities assigned by Executive Order 12344, Naval Nuclear Propulsion Program, codified at 50 United States Code 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. This SD does not apply to Sensitive Compartmented Information (SCI) information systems located at NNSA sites. SCI systems must comply with Director of Central Intelligence Directives or Intelligence Community Directives security policies. The DOE Office of Intelligence and Counterintelligence approves operation of these information systems.

4. BACKGROUND.

This SD was developed using DOE Order (O) 205.1B Change 3, *Department of Energy Cyber Security Program*, dated 4-29-14, as a baseline and is tailored to meet the mission requirements of NNSA. This SD incorporates and requires a CSP consistent with the unified cybersecurity framework outlined in national policies, instructions, standards, and guidelines issued by the CNSS and NIST. This SD also supports the guidance from the National Manager for National Security Systems (NSSs).

Through the implementation of the CSP requirements outlined in this policy, NNSA program offices and their associated field sites, including NNSA laboratories and plants, can effectively meet *Federal Information Security Management Act* (FISMA), *Federal Information Technology Acquisition Reform Act* (FITARA), *Cybersecurity Act* of 2015, and other federal requirements and obligations. In addition, NNSA program offices and their associated field sites can ensure implementation of cost-effective security controls and investments, consistent with DOE/NNSA mission requirements that are in alignment with current threats.

5. REQUIREMENTS.

a. Develop, execute, and maintain a comprehensive CSP that:

(1) Applies and implements a multi-tiered cybersecurity RMF that must meet the following requirements:

(a) Uses Federal Information Processing Standards (FIPS), including FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems* and FIPS 200, *Minimum Security Requirements for Federal Information and Information*

Systems.

(b) Implements CNSS Instruction 1253, *Security Categorization and Control Selection for National Security Systems* (NSS), requirements for all classified systems, including NSS, and other CNSS Issuances, as applicable. See Attachment C for a table mapping DOE information to CNSS Potential Impact Levels.

(c) Implements cybersecurity protections based on requirements specified in Department of Homeland Security (DHS) Binding Operational Directives (BODs) per FISMA, as amended in 2014.

(d) Incorporates and uses all applicable CNSS/NIST guidance.

(e) Protects NNSA information and information assets in a manner commensurate with mission importance, significance to national security, threat capability, known vulnerabilities, and consequence of its loss or compromise, and allocates resources to reduce risk.

(f) Applies federally approved configuration baselines that have been permitted by the Authorizing Official (AO). Exceptions to enterprise systems require final approval from the enterprise AO.

i. Specialized systems will be addressed by the element AO.

ii. The element AO may add, but not reduce, requirements without working through the exception process.

(2) Protects United States' interests and NNSA operational capabilities, individuals, organizations, and assets from the NNSA enterprise level, through the element level, down to the information system level as described in CNSS Policy 22, Cyber Risk Management, August 2016.

(3) Maintains a cost effective and secure environment, which will enable the organization to perform and meet its mission and business operations, goals, and objectives.

(4) Aligns the RMF with NIST Special Publication (SP) 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View* and NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*.

(5) Ensures risks associated with vulnerabilities inherent to information technology (IT), global sourcing and distribution, and adversary threats to organization use of cyberspace must be considered in employment of capabilities to achieve objectives in business operations.

(6) Implements and maintains information security configurations and vulnerability management as it relates to information, IT, and NSSs.

(7) Establishes roles, responsibilities, communications, and risk reporting structures based on this SD and NIST publications.

(8) Establishes a risk strategy and risk tolerance threshold based on the criticality of organizational mission and business functions.

(9) Supports the objectives and goals of the NNSA Strategic Vision.

(10) Integrates cybersecurity into business and mission IS lifecycles.

(11) Provides the flexibility to tailor and implement risk mitigation controls in light of local threats, acceptable risks, mission needs, and environmental and operational factors.

(12) Manages interconnections of business and mission ISs to minimize shared risk by ensuring that the security posture of one system is not undermined by vulnerabilities of interconnected systems.

(a) Memorandum of Understandings/Agreements are not required for any system interconnections between NNSA systems.

(b) Security agreements may not be required for limited interconnection through perimeter defenses that do not expose the protected internal network to significant increase in risk, and are between NNSA entities.

(13) Employs cybersecurity defenses to protect, detect, characterize, counter, and mitigate unauthorized activity and vulnerabilities on ISs. Actively evaluates, responds to, and mitigates changing threats and evolving situations to continuously maintain risk at acceptable levels as defined in site risk management plans and the enterprise threat tolerance statement levels. Also, ensures that information is shared with all authorized personnel in support of DOE/NNSA enterprise-wide situational awareness and operations decisions.

(14) Incorporates Federal Risk and Authorization Management Program (FedRAMP) requirements for establishing and implementing cloud services in accordance with the direction in the NNSA Chief Information Officer's (CIO) Memorandum, *NNSA Cloud Computing Guidance*, dated August 26, 2014. See Attachment B for the requirements of the Memorandum.

(15) Leverages existing or enterprise cybersecurity risk solutions unless the approach does not address the varying mission needs, encounters significant technical barriers, or is not cost effective for implementation. Investments in alternative solutions must document a rationale based on

varying mission needs, significant technical barriers, or cost effectiveness.

(16) Requires annual assessments on the CSP. The Management and Operating contracts (M&Os) performance will be assessed against their Performance Evaluation and Measurement Plans (PEMPs) and provide formal and Fee Determination Official (FDO) approved feedback to the M&Os.

(17) Uses the NNSA approved Enterprise Governance, Risk, and Compliance (EGRC) tool(s) to the fullest extent possible and as defined by guidance issued by the Associate Administrator for Information Management (NA-IM) unless instructed otherwise by the Chief Information Security Officer (CISO) or enterprise AO. Therefore, sites must use cybersecurity diagnostic and mitigation tools that will interface with the EGRC.

(18) Evolves such that Ongoing Authorizations (OAs) are integrated into the CSP. For new information systems, or major modifications to existing ones, the following conditions must be satisfied along with any other criteria as determined by the appropriate AO prior to transitioning to OAs:

(a) An approved pilot has been completed and undergone an independent evaluation.

i. The pilot must include a continuous monitoring program that addresses any changes to hardware, software, personnel, or threat and operational environment (including policies and procedures) in a dynamic environment.

ii. The pilot must document and test the design and operation of a system that provides near real-time security status of changes made to baseline conditions.

(b) The IS must have an approved baseline configuration.

(c) The IS must have a valid Authority to Operate (ATO).

(d) The IS must have a Common Control Catalog in place or develop and implement one.

(e) The IS must have an effective continuous monitoring program within an RMF such that any changes to the information system or its environment are systematically identified and evaluated. The Continuous Monitoring program reporting must include data feeds from Continuous Diagnostics Mitigation tools and controls.

(f) The IS must set up an operational Site Risk Management Council (SRMC).

(g) The IS must provide a training program regarding the new

processes and procedures under an ongoing authorization program to ensure it is effectively implemented and operational.

(19) Requires all Official Use Only (OUO) be controlled appropriately according to DOE O 471.3, Identifying and Protecting Office Use Only Information, DOE M 471.3-1, *Manual for Identifying and Protecting Official Use Only Information*, and DOE O 470.4B, *Safeguards and Security Program*.

(a) IT systems that store OUO information will be certified and accredited for operation in accordance with federal and DOE standards.

(b) Electronic transmission of OUO information, e.g., voice, data or facsimile, and email, shall be protected by encryption and transmitted by systems using other protective measures such as encryption or Public Key Infrastructure (PKI), whenever practical.

(c) Guidance in determining Freedom of Information Act (FOIA) exemptions can be found at http://energy.gov/sites/prod/files/maprod/documents/Wha_is_the_FOIA.pdf.

(20) Establishes requirements that ensures proper control and protection of Controlled Unclassified Information (CUI) identified in 32 Code of Federal Regulations (CFR) Part 2002, *Controlled Unclassified Information*; National Archives and Records Administration's CUI Registry; and 10 CFR Part 1017, *Unclassified Controlled Nuclear Information (UNCI)*. CUI:

(a) Must be controlled, protected, transported, and transmitted in accordance to Executive Order 13556, *Controlled Unclassified Information*; 32 CFR 2002; DOE O 470.4B; and 10 CFR 1017.27, *Transmission*.

(b) Must be protected by encryption when transmitted over telecommunications circuits whenever possible, and protected in a manner that prevents unauthorized access when stored, or in transit via email or telecommunications circuits.

(c) Must be protected consistent with the transmission requirements of 10 CFR 1017.27 guidance if stored on removable media.

(21) Establish an NNSA Telecommunication Security Program. The NNSA Telecommunication Security Program must:

(a) Be effectively established within NNSA as specified in DOE O

470.6, *Technical Security Program* (TSP);

(b) Complement DOE's program such that NNSA requirements are met in a timely and cost-effective manner; and

(c) Be a part of a comprehensive NNSA security program through principles that integrate cybersecurity and physical security requirements. Headquarters (HQ) and site roles and responsibilities will be defined to implement these principles.

(22) Establishes and applies sanitization procedures for media devices that must meet federal requirements and DOE policy. These procedures must be approved by the site AO prior to being implemented.

b. NNSA NSSs must comply with requirements issued by the National Manager for NSS as per Executive Order 13587, *Structural Reform to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, and National Security Directive 42, *National Policy for the Security of National Security Telecommunications and Information Systems*, which concern classified information sharing and safeguarding efforts on computer networks. See Attachment C for additional guidance on Sigma and Restricted data.

c. Supply Chain Risk Management (SCRM) requirements, practices, and processes must be part of the CSP RMA. Requirements must be consistent with existing federal laws, regulations, CNSS instructions or directives, NIST standards and guidelines, Office of Management and Budget (OMB) policies, and other Departmental Directives.

d. Provide cybersecurity training for NNSA elements that use and connect to DOE/NNSA networks and systems. There will be reciprocity between all NNSA sites for this training, and the site only needs to validate the training accomplished. The sites may provide an addendum for the differences in relation to their site, but this should generally be a one or two page read-and-sign.

e. AOs (or their delegate, i.e., Authorizing Official Designated Representative (AODR)) and federal Information System Security Managers (ISSMs) must have Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), or Global Information Assurance Certification (GIAC) certifications or equivalent. Certification requirements must be satisfied within two years of publication of this SD. Acceptance of equivalent certifications must be approved by the CISO. New hires must have the certification or complete it within 120 days of hiring.

f. NNSA information system usage banners, policies, and user agreements must be approved according to direction from the Insider Threat Program Designated Senior Official and meet the minimal standards provided in DOE O 205.1B, Change 3, *Department of Energy Cyber Security Program*.

g. Cybersecurity Program Documentation.

(1) Per DOE O 205.1B, each element must develop a Cybersecurity Implementation Plan. Within NNSA, this SD serves as the NNSA Enterprise Cybersecurity Implementation Plan. The plan:

(a) Will be maintained by the NNSA CIO on behalf of the Administrator;

(b) Will be based on requirements outlined in DOE O 205.1B; and

(c) Will require developing and maintaining appropriate artifacts, such as implementation plans, risk register, and site plans, that support risk decisions.

(2) All CSP practices, procedures, and plans developed within NNSA must be consistent with and incorporate the requirements of this SD.

(3) NNSA sites must develop and maintain comprehensive core documents[1] in support of the RMF implemented for the area of responsibility. The core documents include the Cybersecurity Program Plan (CSPP), Cybersecurity Improvements Plan (CSIP), and Local/System RA Risk Assessment. Sites are also required to maintain this documentation in the EGRC. Additionally, the sites will use the Enterprise Threat Statement in evaluating risk to their site, and are encouraged to use other Enterprise RMF documentation to reduce duplication of effort. Utilization of the enterprise CSPP, and underlying enterprise RMF documentation as it is developed (e.g. ISSPs, RAs, etc.) would reduce effort and cost across the NNSA enterprise.

(a) The CSIP is intended to reflect items that have been identified as representing some degree of risk or that require some type of corrective action. CSIP items may arise from findings identified by external agencies or by internal assessments. CSIP items are typically items that cannot be corrected quickly or require additional resources.

(b) The CSPP is a high-level document detailing the strategies adopted by the site to ensure that effective cybersecurity policies, procedures, and countermeasures are implemented in accordance with federal requirements and risk-based decisions. The CSPP documents the core elements of the NNSA CSP with regard to the electronic processing of both unclassified and classified information for NNSA Enterprise Systems.

[1] Sites may incorporate and maintain the requirements of these core documents as part of other local program plans, policies, standards or procedures.

(c) The Local/System Risk Statement provides an assessment of the greatest risks currently applicable to the agency. NNSA recognizes the importance of these risks, and the impacts they present. With the support of the information within this assessment, the Nuclear Security Enterprise (NSE) can move forward, in collaboration with established risk governance boards, to determine how to further mitigate the identified risks to acceptable levels.

h. Governance.

Must establish a governance board that will oversee NNSA risk management and be governed by leadership, management, and technical experts consisting of the NNSA Management Council, Enterprise Cybersecurity Advisory Board (ECSAB), and Site Risk Management Councils (SRMC).

(a) The NNSA Management Council will govern the CSP.

(b) The ECSAB will be chaired by the Deputy Director for Cyber Security/Enterprise Authorizing Official. Other members include two elected representatives from each site who can effectively communicate information management (IT and Cybersecurity) and mission requirements and essential personnel as designated by the CISO. While sites are addressing inclusion of the requirements of this policy into their contracts, site AOs will serve as representatives on the ECSAB for their respective sites. The ECSAB oversees, advises on, and provides:

i. A common NNSA approach to determine and manage residual risk;

ii. Policy and technology issues relevant to Information Management and Cybersecurity;

iii. Consultation with and feedback to the NNSA CIO and NNSA CISO;

iv. Information sharing among the NSE site risk management councils and the NNSA CIO and NNSA CISO concerning risk management; and

v. Recommendations for an approach and procedures for the NSE for implementing the system-level management and operational and technical controls, further defined in DOE O 205.1B, to supplement the requirements of this SD such as Warning Banners and Plans of Action and Milestones (POA&Ms).

(c) Each site will have an SRMC who will manage information management risks at their respective sites. The SRMC will support the AOs, who are the risk approving and accepting authorities at their respective sites, to manage the risks associated with information systems within their area of responsibility. At sites with M&O contractors, council members are selected to represent the field office and M&O contractor. For HQ, council members are selected by the CISO.

(d) The ECSAB and SRMCs will publish associated charters, define processes, and issue work plans.

6. RESPONSIBILITIES.

a. Administrator.

(1) Retains overall responsibility and accountability for the CSP within the organization, which includes ensuring the development of an NNSA Cybersecurity Implementation Plan. This SD is the NNSA plan.

(2) Serves as a member of the DOE Information Management Governance Board (IMGB) and the DOE Cyber Council. This authority may be further delegated within the organization.

b. NNSA Contracting Officers.

(1) After notification by the appropriate program official, incorporate this SD into the list of applicable directives of affected contracts via the laws, regulations, and DOE Directives clauses of the contracts.

(2) Assist originators of procurement requests who want to incorporate this Directive in new non-site or facility management contracts, as appropriate.

c. Chief, Defense Nuclear Security (CDNS).

(1) Responsible for the development and implementation of security programs for NNSA, including the protection, control, and accounting of materials, and for the physical and cybersecurity for all facilities of NNSA.

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

(1) Supports the Department-wide CSP as directed by the IMGB, by developing and maintaining NNSA's RMF, cybersecurity policies, procedures, to include training materials and threat statements.

(2) Participates in the development and implementation of a Department-wide cybersecurity incident reporting, assessment, and response program.

(3) Provides direction to the NSE pertaining to risk management activities.

(4) Serves as the AO for information systems within NNSA. This authority may be further delegated to qualified appointments within the organization.

(5) Serves as a member of the DOE IMGB.

(6) Assigned as the functional leader for cybersecurity within NNSA, as described in SD 226.1B.

(7) Conducts oversight activities of all NNSA field office's performance in the area of cybersecurity as described in SD 226.1B.

(8) Ensures the integration of cybersecurity with capital planning and investment control, enterprise architecture, and acquisition and system development life cycles.

(9) Ensures the preparation and maintenance of organizational RMFs in the requirements section of this policy.

(10) Appoints the NNSA CISO with approval from the Administrator.

(11) Makes and disseminates to NNSA sites determinations on the Information Condition (INFOCON) level for NNSA.

(12) Serves as the Officially Designated Federal Security Authority (ODFSA) for the NNSA enterprise Telecommunications Security Program. The NNSA Telecommunications Security program consists of the following Technical Security Program Elements:

a. TEMPEST

b. Protected Distribution Systems (PDS)

c. Wireless Security (WISEC)

d. Communications Security (COMSEC)

This authority may be delegated to appointees within the organization who meet the standards set forth in DOE O 470.6, Technical Security Program.

(13) Approves the NNSA enterprise Telecommunications Security Program.

(14) Approves deviations to TEMPEST and PDS policies with the recommendation of the NNSA Certified TEMPEST Technical Authority.

(15) Ensures that information systems have undergone a security authorization process and have received an ATO.

(16) Evaluates issues from the ECSAB and presents those issues to the NNSA Management Council for discussion or resolution.

(17) Notifies the ECSAB of performance or status of issues that are presented to the NNSA Management Council.

(18) Submits risk management tasks to SRMCs to include notifications to the field office based on decisions of the NNSA Management Council.

(19) Facilitates and manages the successful inclusion of hardware and software SCRM practices and processes as part of the RMA. Requirements must be consistent with existing federal laws, regulations, CNSS instructions or directives, NIST standards and guidelines, OMB policies, and other Departmental Directives.

(20) Coordinates with the DOE CIO in cybersecurity incidents, as circumstances warrant, consistent with the standards and guidelines issued by DHS.

(21) Ensures that record management requirements are included throughout the CSP.

(22) Notifies contracting officers which contracts are affected by requirements of this policy.

e. NNSA Chief Information Security Officer (CISO).

(1) Develops, maintains, and manages an NNSA Enterprise CSP to fulfill NNSA's statutory and regulatory cybersecurity responsibilities.

(2) Ensures that security requirements specified in the FISMA are accomplished in an efficient and cost-effective manner.

(3) Serves as the NNSA Cybersecurity Risk Executive as described in NIST SP 800-39.

(4) Ensures that the NNSA cybersecurity architecture supports and enables the NNSA's missions.

(5) Oversees the development, implementation, and management of an NNSA-wide cybersecurity incident management program to include reporting, assessments, and response procedures in coordination with the Office of Environment, Health, Safety and Security; DOE Office of the Chief Information Officer; Defense Nuclear Security; the Nuclear Safeguards and Security organization; Office of Intelligence and Counterintelligence; or Office of Inspector General, as circumstances warrant.

(6) Oversees the establishment and maintenance of a security operation that,

through automated and continuous monitoring, can detect, contain, and mitigate incidents that impair information security and agency information systems.

(7) Ensures development and maintenance of Cybersecurity Implementation Plans.

(8) Manages and provides the NNSA's response for all Agency-level cybersecurity inquiries (e.g., Congressional, DHS, and cybersecurity program review requirements), in coordination with the Joint Cybersecurity Coordination Center (JC3).

(9) Serves as the primary point of contact (POC) for the CIO relative to cybersecurity activities with senior DOE management and other federal agencies.

(10) Prepares and maintains an organizational RMF, to include an NNSA Risk Management Implementation Plan, which consists of site-level Risk Management Implementation Plans and other NNSA risk factors.

(11) Prepares and distributes guidance to the NNSA sites on critical cyber controls, as needed.

(12) Ensures the allocation of sufficient resources to address enterprise cybersecurity risks.

(13) Reviews quarterly and annual program assessment reports resulting from the continuous monitoring component of the RMF and incorporates FDO-approved periodic Interim Feedback Reports and the annual Performance Evaluation Report in order to complete the Information Surety Report or reporting.

(14) Ensures that for NSS, direction from the National Manager is implemented pursuant to Executive Order 13587 and National Security Directive 42.

(15) In conjunction with the NNSA Certified TEMPEST Technical Authority (CTTA), ensures that all of the TSP elements of the NNSA telecommunications security program is funded and implemented according to DOE O 470.6, applicable national policy and the Memorandum of Agreement between the NNSA Office of Defense Nuclear Security and the NNSA Office of the Chief Information Officer regarding the NNSA TEMPEST Program.

(16) Maintains communication between all NNSA elements concerning NNSA risk management activities.

(17) Coordinates the sharing of threat information with senior department managers, the Office of Intelligence and Counterintelligence, NNSA

elements, JC3, and other U.S. Government officials, as needed.

(18) Ensures personnel are sufficiently trained and certified to assist in complying with the information security requirements in relation to legislation, policies, directives, instructions, standards, and guidelines.

(19) Issues guidance and direction in accordance with the requirements outlined in this policy.

(20) Ensures policies are in place to address NNSA Information Condition (INFOCON) level.

(21) Through the most rapid means possible, notifies NNSA elements, through the cognizant AOs, when the NNSA INFOCON level is changed.

(22) Distributes DHS BOD guidance as applicable to NNSA systems and networks.

(23) Reports annually to agency executives the effectiveness of the agency information security program; information derived from automated and continuous monitoring, including threat assessments; and progress on actions to remediate threats.

f. NNSA Enterprise Authorizing Official.

(1) Is the AO responsible for federal oversight and protection of NNSA enterprise systems. This must be a federal employee.

(2) Grants a formal ATO, withdraws authorization, suspends operations, grants interim ATOs, or grants variances when circumstances warrant, in accordance with NIST SP 800-37.

(3) Performs the roles and responsibilities defined for the AO in Appendix D of NIST SP 800-39 for enterprise-wide Federal Government systems under their cognizance.

(4) Delegates responsibilities to an AO Representative, except the authority to grant ATOs.

(5) Is accountable for the security of the information and systems that they authorize.

(6) Implements security guidance issued by NNSA Office of Chief Information Officer (OCIO) and CISO that impacts the risk levels of information systems under their cognizance.

(7) Ensures that documentation is maintained for all information system authorizations under their purview.

(8) Disseminates INFOCON level status changes received from the CISO.

(9) Ensures that all appropriate roles and responsibilities are accomplished as required for each information system.

(10) Ensures that operational information system security policies are communicated for each system, project, program, and site for which the AO has approval authority.

(11) Approves or recommends approval for waivers and exceptions and forwards such information to the NNSA CISO, as appropriate.

(12) Works with the senior site contractor management (i.e., Laboratory Director, Plant Manager) and applicable mission owner(s) to approve acceptable risk and processes.

(13) Oversees the enterprise CSP and risk management activities, using the NSE Integration Assessment Planning Model to meet the oversight and survey responsibilities for the CSP. Ensures adequate resources are allocated to the CSP.

(14) Approves security risk decisions that would exceed the approved risk envelope. This can include making determinations to suspend operations if the risk envelope is exceeded without formal risk acceptance, approval, or choosing to change point of acceptance from RMF to a lower level based on concerns with the associated system or classification or caveats.

(15) Validates budget requirements as associated with enterprise system requirements and the NNSA work breakdown structure process.

(16) Approves all classified Information System Security Plans (ISSPs) within the RMF unless delegated to the ISSM. The ISSM cannot delegate approval authority beyond an alternate.

(17) Ensures federal/DOE/NNSA requirements are flowed into the adopted RMF.

(18) Approves all media clearing, sanitization, and destruction methods.

(19) Ensures all cyber-related incidents affecting NNSA information and information assets are properly reported.

(20) Approves the annual testing (pen test/red/blue team) activity plan and associated tools against NNSA assets and sites.

(21) Approves the continuous monitoring plan and reporting.

(22) Participates in annual training to maintain currency in security technologies

and ensures compliance with Department of Defense (DOD) 8570.01-M *Information Assurance Workforce Improvement Program* for management levels II and III.

(23) Appoints or approves, in writing, an ISSM responsible for implementing federal cybersecurity requirements within the federal systems, as deemed necessary.

(24) Ensures that the site's ISSM, Information System Security Officers (ISSOs), Information System Owners, System Administrators (SAs), and users are trained in their specific duties, and in the technologies for which they have responsibility.

(25) Ensures and facilitates privileged access by properly trained Technical Surveillance Countermeasures (TSCM) technicians and their tools onto NNSA information systems and networks within the area of responsibility.

(26) Ensures data call requirements are met.

(27) Ensures that all appropriate roles and responsibilities are accomplished as required for each information system.

g. Field Office Manager (FOM).

(1) Appoints a qualified senior federal official as the AO for the area of responsibility. The individual must meet certification requirements as defined by the NNSA CISO.

(2) Ensures the development and implementation of the site RMF.

(3) Supports the CISO by providing a representative(s) to support the NNSA Cybersecurity Risk Executive, when requested.

(4) Ensures appointment of a contractor representative to participate on the ECSAB in conjunction with the site/element AO who serves as a default member.

(5) Ensures appointment of members of the SRMC in conjunction with the Senior Site Contractor Management and mission owners. Sites that fall under the purview of HQ will coordinate with CISO on appointment of council members.

(6) Appoints a qualified senior federal official to serve as the Officially Designated Federal Security Authority (ODFSA) for Telecommunications Security Program within their area of responsibility.

h. Field Office/Site AO.

(1) Is the AO responsible for federal oversight of M&O site cybersecurity programs and systems under their purview; approves acceptable risk and processes through the site-specific RMF; ensures placement of this policy's requirements, the approved risk and processes into the M&O and support services contract; and ensures contract updates are completed as applicable.

(2) Grants formal ATOs, withdraws authorization, suspends operations, grants interim ATOs, or grants variances when circumstances warrant, in accordance with NIST SP 800-37.

(3) Perform the roles and responsibilities defined for the AO in Appendix D of NIST SP 800-39.

(4) Completes federal AO functions consistent with FISMA and risk management guidance available from DOE and NNSA governance structures.

(5) Assists HQ in moving the organization forward on enterprise endeavors as requested.

(6) Ensures external systems and services provided by M&O or support contractors meet acceptable risk levels in accordance with approved RMF.

(7) Supports the CISO by providing representative(s) to support the NNSA Cybersecurity Risk Executive when requested.

(8) Validates qualifications of individuals appointed as an ISSM.

(9) Ensures appointment of members of SRMC in conjunction with the Senior Site Contractor Management and mission owners. Sites that fall under the purview of HQ will coordinate with NNSA CISO on appointment of council members.

(10) Ensures that records are maintained for all cybersecurity-related vulnerabilities and incidents requiring remediation.

(11) Ensures and facilitates privileged access by properly trained TSCM technicians and their tools onto NNSA information systems and networks within the area of responsibility.

i. Authorizing Official Designated Representative.

(1) Acts on behalf of an AO to coordinate and conduct the required day-to-day activities associated with the security authorization process.

(2) Can be empowered by AOs to make certain decisions with regard to the

planning and resourcing of the security authorization process, approval of the security plan, approval and monitoring the implementation of POA&Ms, and the assessment or determination of risk.

(3) May also be called upon to prepare the final security authorization package, obtain the AO signature on the security authorization decision document, and transmit the security authorization package to appropriate organizational officials.

(4) Advises AO if RMF risk parameters are exceeded or might be exceeded.

Note: Security authorization decision and signing of the associated security authorization decision document (i.e., the acceptance of risk to organizational operations and assets, individuals, other organizations, and the Nation) cannot be delegated to the designated representative by the AO.

j. Information System Security Manager.

(1) Develops, implements, and monitors the federal element's CSP in accordance with the Site Risk Management Plan and Program Execution Guidance (PEG).

(2) Maintains record copies of CSP plans and reports to include ISSP plans for systems under their cognizance.

(3) Ensures written appointments of ISSOs for information systems and ensures site personnel are aware of and fulfill their information security management and user duties as described in the Site Risk Management Plan.

(4) Evaluates incident reports for NNSA Computer Network Attack (CNA), and Computer Network Exploitation (CNE) situations.

(5) Coordinates security-related incident communications between the site and the IARC.

(6) Ensures all cybersecurity-related incidents are reported to the IARC and AO, in accordance with Attachment D.

(7) Develops incident-reporting procedures.

(8) Initiates protective or corrective measures when a security incident or vulnerability is discovered.

(9) Ensures that training is available for information systems, cybersecurity requirements, operations, safeguards, and incident handling procedures.

(10) Ensures examination and documentation of suspected cybersecurity

incidents and retention of documentation.

(11) Ensures analyses of and corrective actions for incidents and findings are included in the status reporting to the AO.

(12) Provides monthly status update reports to the AO, in accordance with Attachment D.

(13) Follows procedures approved by the AO for authorizing software, hardware, and firmware use before implementation on the system.

(14) Conducts periodic reviews to ensure compliance with the CSPP and ISSPs.

(15) Recommends changes to the INFOCON status to the AO. Changes will be based on Incident Response NNSA-IR-07 stated in the NNSA CSPP.

(16) Ensures that training is available for ISSOs and SAs for information systems, cybersecurity requirements, operations, safeguards, INFOCON, and incident handling procedures.

k. Information System Owner.

(1) Responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system in accordance with FITARA and other federal regulations.

(2) Addresses the operational interests of the user community (i.e., users who require access to the information system to satisfy mission, business, or operational requirements) and ensures compliance with information security requirements.

(3) Responsible, in coordination with the ISSO, for the development and maintenance of the security plan and ensures that the system is deployed and operated in accordance with the agreed-upon security controls.

(4) In coordination with the information owner, responsible for deciding who has access to the system (and what types of privileges or access rights) and ensures that system users and support personnel receive the requisite security training (e.g., instruction in rules of behavior).

(5) With authority from the AO, informs appropriate organizational officials of the need to conduct the security authorization; ensures that the necessary resources are available for the effort; and provides the required information system access, information, and documentation to the security control assessor.

(6) Receives the security assessment results from the security control assessor.

(7) After taking appropriate steps to reduce or eliminate vulnerabilities, assembles the authorization package and submits the package to the AO or the AODR for adjudication.

l. Information System Security Officer (ISSO).

(1) Ensures that the appropriate operational security posture is maintained for an information system and, as such, works closely with the information system owner responsible for ensuring that the appropriate operational security posture is maintained for that information system.

(2) Serves as a principal advisor on all matters, technical and otherwise, involving the security of an information system.

m. NNSA Information Assurance Response Center.

(1) Collects, analyzes, and shares cybersecurity information and serves as the NNSA incident response coordination and reporting element.

(2) Reports cybersecurity incidents to the DOE JC3.

(3) Provides enterprise tools, enterprise cyber intelligence, advance analysis, and first responders to incidents.

(4) Coordinates response throughout the Department during significant cybersecurity incident events.

(5) Maintains a current list of Departmental contacts for cybersecurity incident coordination and specialized skills.

(6) Provides alerts and bulletins concerning cyber events to NNSA elements.

(7) Keeps the CISO apprised of events and concerns that have or may have a negative effect on the security state of Departmental information or IT resources.

n. Information Owner.

(1) An organizational official with statutory, management, or operational authority for specified information and the responsibility for establishing the policies and procedures governing its generation, collection, processing, dissemination, and disposal.

(2) Responsible for establishing the rules for appropriate use and protection of the subject information (e.g., rules of behavior) and retains that responsibility even when the information is shared with or provided to other organizations. The owner or steward of the information processed, stored, or transmitted by an information system may or may not be the

same as the system owner. A single information system may contain information from multiple information owners or stewards.

(3) Provides input to information system owners regarding the security requirements and security controls for the systems where the information is processed, stored, or transmitted.

o. The Enterprise Cybersecurity Advisory Board (ECSAB).

(1) Determines risk impacts to the Enterprise CSP.

(2) Provides independent consultation and feedback from the NNSA elements' and Headquarters' perspective to the NNSA CIO.

(3) Develops a common NNSA approach to determine and manage residual risk and reports results to the NNSA CIO.

(4) Advises and coordinates policy and technology issues relevant to IT and Cybersecurity and reports results to the NNSA CIO.

(5) Prioritizes issues to elevate to the NNSA CIO and flags decisions needed from the NNSA CIO/Management Council.

(6) Promotes cooperation, collaboration, and information sharing among the NNSA sites concerning risk management activities to include shared responsibilities for joint and leveraged authorizations and services provided by external providers.

(7) Communicates information and decisions back to sites and appropriate AOs.

(8) Ensures SRMCs are established and operating as required by this SD.

p. Site Risk Management Council (SRMC).

(1) Submits insufficiently mitigated risks and other issues to the ECSAB.

(2) Notifies AOs in regards to communications with the ECSAB information or decision from the NNSA CIO.

7. REFERENCES. See Appendix 2.

8. DEFINITIONS. See Appendix 1.

9. CONTACT. Office of Information Management and Chief Information Officer at (202) 586-9728.

BY ORDER OF THE ADMINISTRATOR:

Frank G. Klotz
Administrator

Attachments:
A. Contractor Requirements Document (CRD)
B. NNSA Cloud Computing FEDRAMP Guidance Memorandum
C. Table Mapping DOE Information Groups to CNSS 1253 Potential Impact Levels
D. Incident Management
E. Transmission of Restricted Data Over Secret Internet Protocol Router Network (SIPRNET)
F. Information Condition (INFOCON)

Appendixes:
1. Definitions
2. References

ATTACHMENT A: CONTRACTOR REQUIREMENTS DOCUMENT
SD-205.1, BASELINE CYBERSECURITY PROGRAM

This Contractor Requirements Document (CRD) establishes the requirements for National Nuclear Security Administration (NNSA) contractors with access to NNSA and Department of Energy (DOE) information systems. Contractors must comply with the requirements listed in this CRD.

The contractor is responsible for complying with and flowing down the requirements of this CRD to subcontractors at any tier to the extent necessary to ensure the contractor's compliance with these requirements. The contractor will ensure that it and its subcontractors comply with the requirements of this CRD and incur only those costs that would be incurred by a prudent person in the conduct of competitive business.

In addition to the requirements set forth in this CRD, contractors are responsible for complying with Attachments B through E to this Policy referenced in and made a part of this CRD and which provide information to assist in the implementation of program requirements applicable to contracts in which this CRD is inserted. The contractor will ensure that it and its subcontractors cost-effectively comply with the requirements of this CRD. The Contractor must:

1. Ensure NNSA information and information assets are protected in a manner commensurate with mission importance, significance to national security, threat, vulnerability, and magnitude of harm relative to compromise.

2. Ensure NNSA National Security Systems (NSSs) comply with requirements issued per Executive Order 13587, S*tructural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, and National Security Directive 42, *National Policy for the Security of National Security Telecommunications and Information Systems*, which concern classified information sharing and safeguarding efforts on computer networks.

3. Develop and maintain a comprehensive Cybersecurity Program (CSP) that applies and implements a multi-tiered cybersecurity Risk Management Framework (RMF) and meets the following requirements:

    a. Implements Committee on National Security Systems (CNSS) Instruction 1253, *Security Categorization and Control Selection for National Security Systems*, requirements for all classified systems and other CNSS Issuances, as applicable, for National Security Systems.

    b. Incorporates applicable National Institute of Standards and Technology (NIST) Special Publication (SP) documentation for the cyber program.

    c. Must implement Federal Information Processing Standards (FIPS) 199, S*tandards for Security Categorization of Federal Information and Information Systems*, and FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, for unclassified and classified systems and CNSS

requirements for national security systems. Correct system categorization will be added to NNSA site inspection agendas to ensure consistent security impact assessments across NNSA.

d. Maintains a cost effective and secure environment, which will enable the organization to perform its mission and meet its business goals.

e. Aligns with the NNSA Enterprise RMF, NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, and NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*.

f. Uses the NNSA Enterprise Threat and the Local/System Risk Statement as a core document to prioritize and address risks to business and mission operations. Prioritization shall consider likelihood, consequence, and residual risk as described in the threat statement.

g. Ensures risks associated with vulnerabilities inherent in Information Technology (IT), global sourcing and distribution, and adversarial threats to organizational use of cyberspace be considered in employment of capabilities to achieve objectives in business operations.

h. Establishes sanitization procedures for media devices to meet federal requirements and policy compliance with approval by the responsible Authorizing Official (AO).

i. Establishes a risk strategy based on the criticality of organizational mission and business functions.

j. Supports the goals and objectives of the NNSA *Enterprise Strategic Vision*.

k. Fully integrates cybersecurity into business and mission information system (IS) lifecycles.

l. Protects DOE/NNSA information and information assets in a cost-effective manner by managing cybersecurity risks, considering mission priorities, and allocating resources to the most efficient solutions necessary to reduce risk to acceptable levels.

m. Provides the flexibility to tailor and implement security programs and risk mitigation controls in light of local threats, acceptable risks, mission needs, and environmental and operational factors.

n. Manages interconnections of business and mission IS to minimize shared risk by ensuring that the security posture of one system is not undermined by vulnerabilities of interconnected systems.

o. Employs cybersecurity defenses to protect, detect, characterize, counter, and

mitigate unauthorized activity and vulnerabilities on ISs. Also, actively evaluates, responds to, and mitigates changing threats and evolving situations to continuously manage risk to acceptable levels as defined in site risk management plans and the enterprise threat tolerance statement levels. Ensures that information from cybersecurity defenses is shared with personnel with appropriate clearance and a need-to-know, in support of DOE/NNSA enterprise-wide situational awareness.

p. Implements cybersecurity protections based on requirements specified in Department of Homeland Security (DHS) Binding Operational Directives (BOD). Requirements from any applicable DHS BOD will be determined by the AO and communicated to the Management and Operating contract (M&O) through the contracting official.

q. Incorporates Federal Risk and Authorization Management Program (FedRAMP) requirements for establishing and implementing cloud services for federal information systems. See Attachment B for FedRAMP requirements.

r. Must use cybersecurity risk solutions that will interface with the Enterprise Governance, Risk, and Compliance (EGRC) tool to the fullest extent possible as defined by NNSA Associate Administrator for Information Management (NA-IM) guidance. The EGRC is the official corporate/enterprise program repository that will be used to perform continuous performance monitoring and reporting of information security program management, operations and technical controls (i.e., ATO packages, deviations, incident management reporting). Therefore, sites must use cybersecurity diagnostic and mitigation tools that will interface with the EGRC.

s. Leverages existing or enterprise cybersecurity risk solutions as documented in the EGRC, unless the approach does not address the varying mission needs, encounters significant technical barriers, or is not cost effective for implementation.

t. Must implement guidance provided by NNSA Headquarters (HQ) as it relates to critical cyber activities.

u. Requires annual assessments of the CSP. The M&Os performance will be assessed against the Performance Evaluation and Measurement Plans (PEMPs) and provide formal feedback to the M&Os.

v. Ensures the implementation of a framework for the Planning, Programming, Budgeting, and Evaluation (PPBE) process and allocation of resources with the cybersecurity program.

4. Each site will have a Site Risk Management Council (SRMC). These site-level councils will manage information management risks at their respective sites. Additionally, these councils will support the federal appointed AOs, who are the risk approving and

accepting authorities at their respective sites, to manage the risks associated with information systems within their area of responsibility.

5. Cybersecurity Program Assurance.

   a. In the context of M&O contractors, the approach adopts and uses the flexibility and tailoring described above and includes focus on federal oversight of high-level balanced outcomes and outputs of the Contractor Assurance Systems (CAS), and the contractor's performance in meeting cybersecurity expectations as defined in SD 226.1B, *NNSA Site Governance*.

   b. Information System Security Managers (ISSMs) must have a Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), or Global Information Assurance Certification (GIAC) certification or equivalent. Equivalence must be approved by the Chief Information Security Officer (CISO). Personnel in the position currently without the certification must obtain the certification within two years of publication of this document. New hires must have the certification or obtain it within 120 days of hiring.

   c. Contractor Assurance Systems must provide quarterly CSP and performance reporting in accordance with direction from the NNSA CISO covering the following elements:

      (1) Site Cybersecurity Program Performance, and

      (2) Site Cybersecurity Budget.

6. Controlled Unclassified Information (CUI).

   a. Establishes requirements that ensure proper protection of Controlled Unclassified Information (CUI) identified in National Archives and Records Administration's CUI Registry categories and subcategories, and 10 CFR Part 1017, *Identification and Protection of Unclassified Controlled Nuclear Information* . CUI:

      (1) Must be controlled, transported, and transmitted according to Executive Order 13556, *Controlled Unclassified Information*; DOE O 470.4B, *Safeguards and Security Program*; 32 CFR 2002, *Controlled Unclassified Information*; and 10 CFR 1017.27, *Transmission*. Guidance in determining Freedom of Information Act (FOIA) exemptions can be found at http://energy.gov/sites/prod/files/maprod/documents/Wha_is_the_FOIA.

      (2) Must be protected by encryption when transmitted over telecommunications circuits whenever possible, and protected in a manner that prevents unauthorized access when stored or in transit.

      (3) Must be protected consistent with the transmission requirements of 10

CFR 1017.27 guidance if stored on removable media.

(4) Must be controlled appropriately according to DOE O 471.3 Admin Change 1, *Identifying and Protecting Official Use Only Information*; DOE M 471.3-1 Admin Change 1, *Manual for Identifying and Protecting Official Use Only Information*; and DOE O 470.4B Admin Change 1, *Safeguards and Security Program*.

(5) Must also be treated as sensitive, be protected by encryption when transmitted over telecommunications circuits whenever possible, and be protected in a manner that prevents unauthorized access when stored or in transit per DOE M 471.3-1 guidance. Guidance on personally identifiable information (PII) can be found in DOE O 206.1, *DOE Privacy Program.*

b. Guidance in determining Freedom of Information Act (FOIA) exemptions for OUO can be found at http://energy.gov/sites/prod/files/maprod/documents/Wha_is_the_FOIA.pdf

7. Cybersecurity RMF Documentation.

a. NNSA site must develop and maintain these comprehensive core documents in support of the RMF implemented for the area of responsibility. The core documents include the Cybersecurity Program Plan (CSPP), Cybersecurity Improvements Plan (CSIP), and Local/System RA Risk Assessment. Sites are also required to maintain this documentation in the EGRC. Additionally, the sites will use the Enterprise Threat Statement in evaluation of risk to their site, and are encouraged to use other Enterprise RMF documentation to reduce duplication of effort. Utilization of the enterprise CSPP, and underlying enterprise RMF documentation as it is developed (e.g., ISSPs, RAs, etc.) would reduce effort and cost across the NNSA enterprise as a whole.

(1) The CSIP is intended to reflect items that have been identified as representing some degree of risk or that require some type of corrective action. CSIP items may arise from findings identified by external agencies or by internal System Administrators (SAs). CSIP items typically cannot be corrected quickly or require additional resources.

(2) The CSPP is a high-level document detailing the strategies adopted by the site to ensure that effective cybersecurity policies, procedures, and countermeasures are implemented in accordance with federal requirements and risk-based decisions. The CSPP documents the core elements of the NNSA Cybersecurity Program (CSP) with regard to the electronic processing of both unclassified and classified information for NNSA Enterprise Systems.

(3) Local/System Risk Statement provides an assessment of the greatest risks currently applicable to the agency. NNSA recognizes the importance of

these risks and the impacts they present. With the support of the information within this assessment, the nuclear security enterprise (NSE) can move forward, in collaboration with established risk governance boards, to determine how to further mitigate the identified risks.

b. The contractor ISSM must establish and maintain an incident management and reporting capability that is consistent with NIST guidance. This capability must include:

(1) Reporting cybersecurity and privacy incidents to the Information Assurance Response Center (IARC) in accordance with Attachment D.

(2) Requirements to immediately report any suspected loss or unauthorized exposure of information associated with NSSs. The incident must be immediately reported to the AO and the IARC.

8. Roles and Responsibilities.

a. Senior Site Contractor Manager.

(1) Leads the process in conjunction with the Site Office Manager and the mission owners to set an acceptable risk level for those information assets under their purview in a Site Risk Management Plan.

(2) Ensures the laboratory or plant develops and maintains a comprehensive CSP employing an RMF based on the acceptable risk level identified in the Site Risk Management Plan that is approved by the federal appointed site AO.

(3) Ensures the laboratory or plant develops a CAS based on the requirements outlined in SD 226.1B, *NNSA Site Governance*, and the requirements of this policy.

(4) Ensures appointment of a contractor representative to participate on the ECSAB in conjunction with the Field Office Manager (FOM) and federal appointed site AO who serves as a default member.

(5) Ensures establishment of SRMC and appointment of council members in conjunction with the M&O CIO, FOM, and federal appointed site AO.

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

(1) Assists the Senior Contractor Official with developing and maintaining a comprehensive CSP, including site management roles and responsibilities as well as an RMF and CAS.

(2) Assumes full accountability for site execution of an effective CSP.

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

(4) Ensures the appointment of an ISSM to be responsible for direct oversight of development and implementation of the CSP at the M&O site.

(5) Will validate the qualifications of an individual appointed as an ISSM in collaboration with the AO.

(6) Ensures establishment of SRMC and appointment of council members in conjunction with the Senior Site Contractor Manager, FOM, and federal appointed site AO.

(7) Serves as a senior subject matter expert (SME) on SRMC.

c. Contractor Information System Security Manager.

(1) Develops, implements, and monitors the M&O CSP in accordance with the Site Risk Management Plan approved by the federal appointed site AO and Program Execution Guidance (PEG).

(2) Maintains records of the M&O's CSP plans and reports to include Information Systems Security Plans (ISSPs) for systems under their cognizance.

(3) Ensures written appointments of Information System Security Officers (ISSOs) for information systems operated by their respective NNSA M&O and site personnel are aware of and fulfill their cybersecurity management and user duties as prescribed by the RMF documented in the Site Risk Management Plan.

(4) Ensures that records are maintained for all cybersecurity-related vulnerabilities and incidents requiring remediation.

(5) Serves as a senior SME on SRMC.

THIS PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT B: NNSA CLOUD COMPUTING FEDRAMP GUIDANCE MEMORANDUM

In addition to the requirements set forth in the Contractor Requirements Document (CRD), contractors are responsible for complying with Attachment B to this Policy. This Attachment provides more detailed information and requirements that are also applicable to federal employees.

In accordance with the Office of Management and Budget (OMB) Memorandum, *Security Authorization of Information Systems in Cloud Computing Environments*, dated 12-8-2011, https://cio.gov/wp-content/uploads/2012/09/fedrampmemo.pdf packages may leverage previously assessed cloud services as long as they are reviewed and approved according to the Federal Risk and Authorization Management Program (FedRAMP) process described in the FedRAMP Concept of Operations (CONOPS).

Cloud service providers that have not been FedRAMP-certified must follow the FedRAMP security assessment process per the FedRAMP CONOPS. Exceptions to granting an ATO to a non-FedRAMP provider must be worked through the site/enterprise Authorizing Official (AO).

All approved ATO packages that leverage cloud services need to be forwarded to the National Nuclear Security Administration (NNSA) Office of Chief Information Officer (OCIO) in electronic format.

Currently, public cloud services are only authorized to operate within the low or moderate category levels for systems. The level is based on their FedRAMP certification.

Where a cloud service does not have FedRAMP approval, the site AO will be responsible for working through development of the ATO package. One of the key elements for this will be a review to ensure there is not an approved FedRAMP service provider for the service. In all cases, if a FedRAMP approved provider is available, it will be selected.

This guidance does not change any current contract arrangements, but upon expiration of the contract, the site will pursue an approved FedRAMP provider. Exceptions must be approved by the AO.

If cloud services are needed that are not available through an approved FedRAMP provider, the site AO will perform the approval package assessment and approval for usage. The assessment must have a strong justification for why it is allowed to be used and include documented information sensitivities with associated risk of loss and mitigations. This approval package will be forwarded to the Associate Administrator for Information Management and Chief Information Officer (NA-IM/CIO) in a searchable electronic format.

As with any ATO, the AO must be aware of all risks when authorizing cloud services.

The AO should endeavor to understand not only what functionality they will receive when using a cloud service, but also how the deployment model a cloud service uses will affect the

environment in which government data is placed and the confidentiality of data, as determined by the sensitivity of the data.

As we work through cloud service approvals, NA-IM will work with field site AOs to help identify cloud services where an enterprise ATO may be more beneficial to the nuclear security enterprise versus each site working through the process independently. This addresses one of the key elements of the FedRAMP benefit – reusing a service without each site repeating the work.

ATTACHMENT C: TABLE MAPPING DOE INFORMATION GROUPS TO CNSS 1253 POTENTIAL IMPACT LEVELS

In addition to the requirements set forth in the Contractor Requirements Document (CRD), contractors are responsible for complying with Attachment C to this Policy. This Attachment provides more detailed information and requirements that are also applicable to federal employees.

Table 1-Mapping DOE Information Groups to CNSSI 1253 Potential Impact Levels

DOE Information Group [1]			CNSSI 1253 Potential Impact for Loss of Confidentiality
Confidential (NSI)			Low
Confidential RD[2]			Moderate
Confidential RD [4]	Sigma	1,2,3,4,5,9,10,11,12, and 13	Moderate
Secret (NSI)			Moderate
Secret RD			Moderate to High
Secret RD [3]	Sigma	15 and 18	Moderate to High
Secret RD [3]	Sigma	14 and 20	High
Top Secret (NSI) Top Secret RD [3]		14, 15 18 and 20	High

[1] Potential levels of impact for Integrity and Availability are determined by use of the data as specified by the Information and Information System Owner as part of the Information System Categorization process of Committee on National Security Systems Instruction (CNSSI) 1253.

[2] Restricted Data (RD) restrictions described in the *Atomic Energy Act* of 1954 (as amended) are additional need-to-know access protections, but not additional consequences from authorized disclosure. Unlike National Security Information (NSI), RD category also has no automatic "declassify on date (or event)" as does NSI.

[3] Secret RD, Secret RD with Sigmas, and Top Secret NSI and RD start at the highest CNSSI 1253 potential impact for loss of confidentiality. The initial system categorization level may be adjusted using the site Risk Management Framework (RMF) in accordance with Paragraph 2.1.3 of CNSSI 1253.

[4] Refer to Department of Energy (DOE) O 452.8, *Control of Nuclear Weapon Data* for handling unmodified legacy Nuclear Weapon Data.

Note: For additional direction on authorization/control requirements for the RD category, that includes

Sigma data, see DOE O 452.7, *Protection of Use Control Vulnerabilities and Designs*; DOE O 452.8, *Control of Nuclear Weapon Data*; and DOE O 457.1A, *Nuclear Counterterrorism*.

ATTACHMENT D: INCIDENT MANAGEMENT

In addition to the requirements set forth in the Contractor Requirements Document (CRD), contractors are responsible for complying with Attachment D to this Policy. This Attachment provides more detailed information and requirements that are also applicable to federal employees.

1. INTRODUCTION. This attachment establishes the minimum criteria and processes for reporting and responding to cybersecurity incidents involving National Nuclear Security Administration (NNSA) information systems.

2. SCOPE. The scope of this attachment includes NNSA information and information systems operated by federal personnel and contractors.

3. REPORTING CRITERIA AND PROCESSES.

   a. The site's Cybersecurity Program Plan (CSPP) must document the process for reporting cybersecurity incidents to the Information Assurance Response Center (IARC) that pose an immediate danger or short-term threat or a near- or long-term threat to national security interests or critical NNSA or Department of Energy (DOE) assets. All cybersecurity incidents involving both unclassified and classified information or information systems, including privacy breaches, under NNSA federal or contractor control must be identified, mitigated, categorized, and reported to the IARC. The IARC must be informed of all reportable cybersecurity incidents as specified below. Cybersecurity-related incidents must also be coordinated with Safeguards and Security.

      (1) Incident Types.

         (a) Malicious Code. All instances (successful and attempted) of infection by malicious code, (viruses, Trojan horses, worms), must be reported.

         (b) Loss, Theft, or Missing Equipment and IT Resources. All instances of the loss, theft, or missing laptop computers and information technology (IT) resources, including media, which contain Sensitive Unclassified Information (SUI) or national security information must be reported.

         (c) Personally Identifiable Information (PII). Information collected or maintained by the Department about an individual including, but not limited to, education, financial transactions, medical history, and criminal or employment history, and information that can be used to distinguish or trace an individual's identity. These include name, Social Security Number (SSN), date and place of birth, mother's maiden name, biometric data, and any other personal information linkable to a specific individual.

(d) Phishing. The attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) for malicious reasons, by masquerading as trustworthy in an electronic communication.

(e) Attempted Intrusion. A significant or persistent attempted intrusion that stands out above the daily activity or noise level, as determined by the system owner, and that would result in unauthorized access (compromise) if the system were not protected.

(f) Classified Spillage. Transfer of classified or sensitive information to unaccredited or unauthorized systems, individual's applications, or media. Spillage may result from improper handling of compartments, releasability controls, privacy data, or proprietary information.

(g) Denial of Service (DoS). Intentional or unintentional denial of service (successful or persistent attempts) that affects or threatens to affect a critical service or that denies access to one or more large portions of a network must be reported.

(h) Compromise or Intrusion. All unintentional or intentional instances of system compromise or intrusion by unauthorized persons must be reported, including user-level compromises, root (administrator) compromises, and instances in which users exceed privilege levels.

(i) Unauthorized Use. Unauthorized use should be construed as any activity that adversely affects an information system's normal, baseline performance or is not recognized as being related to NNSA's mission. For example, unauthorized use can be using a DOE or NNSA computer to obtain government data without authorization or using systems to break the law. Unauthorized use can also include, but is not limited to, port scanning that excessively degrades performance.

Note that these activities may only be performed when authorized by the Authorizing Official (AO): IP (Internet protocol) spoofing; network reconnaissance; monitoring; hacking into servers; running traffic-generating applications that generate unnecessary network broadcast storms or push large amounts of traffic to computers; or using illegal (or misusing copyrighted) software images, applications, data, and music.

(2) Impact Classifications. Impact classification characterizes the potential impact of incidents that compromise DOE or NNSA information and

information systems. Such incidents may affect DOE or NNSA operations, assets, individuals, missions, or reputations. The impact analysis below is a fundamental step in risk assessment.

(a) Functional Impact.

i. HIGH. Organization has lost the ability to provide all critical services to all system users.

ii. MEDIUM. Organization has lost the ability to provide a critical service to a subset of system users.

iii. LOW. Organization has experienced a loss of efficiency, but can still provide all critical services to all users with minimal effect on performance.

iv. NONE. Organization has experienced no loss in ability to provide all services to all users.

(b) Information Impact.

i. CLASSIFIED. The confidentiality of classified information was compromised.

ii. PROPRIETARY. The confidentiality of unclassified proprietary information, such as protected critical infrastructure information (PCII), intellectual property, or trade secrets was compromised.

iii. PRIVACY. The confidentiality of personally identifiable information (PII) or personal health information (PHI) was compromised.

iv. INTEGRITY. Information was modified without authorization.

(c) Recoverability.

i. REGULAR. Full recovery time with existing resources is normal.

ii. SUPPLEMENTED. Time to full recovery is estimated longer than normal due to resource limitations.

iii. EXTENDED. Time to full recovery is estimated longer than normal due to resource limitations and outside help is needed.

iv. NOT RECOVERABLE. Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly).

v. NOT APPLICABLE. Incident does not require recovery.

vi. NONE. No information was exfiltrated, modified, deleted, or otherwise compromised.

b. Cybersecurity Incident Reporting Process Requirements. All incidents involving either unclassified or classified NNSA information systems must be reported within an hour of detection and all records must be maintained. Incident management processes and procedures are also to be included in Contingency Plan testing and integrated with PII incident reporting, Information Condition (INFOCON) processes and procedures, and each information system Contingency Plan.

(1) When a cybersecurity incident has occurred or is suspected to have occurred (potential incident), the facts and circumstances surrounding the event must be immediately documented.

(2) Once it is determined that an incident has occurred, the incident must be categorized according to the impact classifications, and reported to the IARC within one hour. The initial investigation is to be completed within 24 hours. Incident notification reports must be sent to iarc@iarc.nv.gov. If incident notification reports are classified, the reports must go through the classified medium as follows to the IARC: iarc@iarc.doe.sgov.gov.

(3) The IARC is responsible for reporting to JC3, as they serve as the top-level NNSA organization responsible for reporting incidents to JC3. The IARC will report positive identification of the incident within the requested one hour period to the JC3. Evaluations of incidents and potential incidents must be documented and local files retained.

(4) Cybersecurity incidents reported to the IARC need to include as much of the following information as possible:

(a) SCENARIO – Indicate whether Ticket Submission Form or Request for Services.

(b) REPORTING OFFICE – Indicate site name and contact information for individual(s) reporting Incident/requesting services. Contact information should include first and last name, phone number, email address, and state.

(c) INCIDENT DETAILS – Indicate as follows:

i. Incident Type: Attempted Intrusion, Classified Spillage, DoS, Loss, Theft, or Missing Equipment and IT Resources, Malicious Code, Phishing, PII, Successful Intrusion, Unauthorized Use, Unknown, or other.

ii. Threat Vectors:

- Attrition (an attack that employs brute force methods to compromise).
- Web (an attack executed against a website or web-based application).
- Email (an attack executed via an email message or attachment).
- External/Removable Media (an attack executed from removable media or a peripheral device).
- Impersonation (an attack involving replacement of legitimate content/services with a malicious substitute).
- Improper Usage (any incident resulting from violation of an organization's acceptable usage policies by an authorized user).
- Loss or Theft of Equipment (the loss or theft of a computing device or media used by the organization).
- Unknown (this is acceptable if cause is unknown upon initial report). The threat vector may be updated in a follow-up report.
- Other (an attack does not fit into any other vector).

iii. Whether the confidentiality, integrity, or availability of information systems were affected.

iv. Date and time, including time zone, incident occurred.

v. Date and time, including time zone, incident was detected.

vi. Incident Description.

vii. Related indicators (e.g., hostnames, domain names, network traffic characteristics, registry keys, X.509 certificates, MD5 file signatures).

viii. Source (i.e., attacking IP address, attacking port, attacking protocol, source date stamp, source timestamp).

ix. Functions of systems impacted (e.g., web server, domain controller, or workstation).

x. Physical location of systems impacted (e.g., city and state)

xi. Source, methods, or tools used to identify the incident.

xii. FUNCTIONAL IMPACT – Indicate as follows:

- The functional impact to the site/agency.
- Number of systems impacted.
- Number of impacted PII records.
- Total number of users impacted.
- Operating systems (OS), including versions, impacted.

xiii. INFORMATION IMPACT – Indicate as follows:

- If the confidentiality of classified information was compromised.
- If sensitive/proprietary/privacy information was infiltrated, exfiltrated, modified, or deleted.
- The types of information compromised.

xiv. RECOVERABILITY/MITIGATION – Indicate as follows:

- Indicate the recoverability for the incident (e.g., Regular, Supplemented, or Extended).
- Number of labor hours used to investigate and remediate the incident.
- Number of staff required to support investigation and remediation efforts.
- If external assistance is required for mitigation.
- Details of the Recovery/Mitigation actions required.
- Details of the Recovery/Mitigation actions completed with associated completion dates.

(5) The Information System Security Manager (ISSM) must be notified immediately of the discovery of an incident by the NNSA site.

(6) The AO will be included on incident notices transmitted to the ISSM/IARC.

(7) The AO will ensure the FOM and NA-IM senior officials are informed of all incidents the results of which may have a significant negative affect to

operations, assets, individuals, missions, or reputations.

(8) The AO will verify that all events are reported to the IARC.

(9) Monthly reports on the status of incident resolution, whether or not any reportable, successful, or attempted incidents have occurred during the month, must also be transmitted to the ISSM. The AO will be included on these reports.

(10) All NNSA sites must fully define and maintain current incident reporting requirements and procedures within their local policy and procedures.

c. Incidents of Security Concern (IOSC). Any cybersecurity incident involving the loss, theft, compromise, or suspected compromise of classified or controlled unclassified information must also be reported through the IOSC program in accordance with DOE O 470.4B, *Safeguards and Security Program*.

d. Archiving Cybersecurity Incident Information. Sites must store all information related to a reportable incident, as defined in paragraph 2.a of this attachment, for at least one year. Storage methods, including custody, must comply with applicable evidentiary requirements for possible law enforcement use.

e. Counterintelligence Reporting. Events identified in DOE O 475.1, *Counterintelligence Program*, must be reported by the IARC to the Office of Intelligence and Counterintelligence (OICI), in accordance with the reporting procedures in DOE O 475.1.

f. Automated Systems. Automated systems may be used to implement these protocols.

4. CYBERSECURITY ALERTS. Cybersecurity alerts issued by JC3 and received by the IARC shall be investigated, analyzed, and reported as an incident, as appropriate. The alerts will be coordinated with the sites as needed to determine reporting requirements. Positive feedback from the sites is required in response to an alert with the incident reporting mechanism providing the necessary information.

THIS PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT E: TRANSMISSION OF RESTRICTED DATA OVER THE NNSA SECRET NETWORK (NSN)

In addition to the requirements set forth in the Contractor Requirements Document (CRD), contractors are responsible for complying with Attachment E to this Policy. This Attachment provides more detailed information and requirements that are also applicable to federal employees.

1. PURPOSE. To establish requirements and responsibilities for operation of the National Nuclear Security Administration (NNSA) Secret Network (NSN) Controlled Interface for the electronic transmission of Restricted Data (RD) between NNSA information systems and NSN.

2. APPLICABILITY.

   a. All entities, federal or contractor, that collect, create, process, transmit, store, or disseminate information on the NSN for NNSA.

      Note: NNSA Headquarters (HQ) Organizations, field offices, Management and Operating (M&O) contractors, integrating contractors, and subcontractors hereafter are referred to as NNSA elements.

   b. Information System. This Attachment applies to any NNSA information system that collects, creates, processes, transmits, stores, or disseminates classified NNSA information. It applies to any information system life cycle, including the development of new information systems, the incorporation of information systems within the infrastructure, the incorporation of information systems outside the infrastructure, the development of prototype information systems, the reconfiguration or upgrade of existing systems, and legacy systems.

3. REQUIREMENTS.

   a. Restricted Data, except for Sigmas 14, 15, 20, and Top Secret, must be transmitted via NSN from a system that has been formally accredited to process, store, and transmit RD information.

   b. NNSA elements must ensure that RD is transmitted only as an encrypted attachment to an e-mail. In addition, all data must be encrypted with a National Security Agency (NSA) type 1 encryption technology.

   c. Restricted Data must not be transmitted in the body of an e-mail.

   d. The requirements and implementation of this Policy must be merged into the Information System Security Plan (ISSP) of an NNSA classified information system, and be subjected to the NNSA Assessment and Authorization Process. The ISSP will include a description of the controlled interface technical and procedural agreements required for transmission, including clearance and briefings required for access to specific classification levels and categories of

information, between the NNSA system and NSN. The interconnection must be part of the Security Test and Evaluation Plan of the Assessment and Authorization process.

e. This section describes the requirements for interconnecting the Department of Defense (DOD) Secret Internet Protocol Router Network (SIPRNet) and a Department of Energy (DOE) system or network accredited for confidential or secret RD.

(1) The access authorization process must incorporate need-to-know and access briefings. The need-to-know and briefings must be validated by the Authorizing Official (AO). The sender and DOD recipients cannot validate the information.

(2) Access authorizations must be re-validated at least monthly to ensure that they remain current.

(3) Processes must be established to ensure the following:

(a) A review and verification of the e-mail content, including attachments transmitted or received via this controlled interface, must be done to ensure that the e-mail does not contain RD that is unencrypted.

(b) All RD transmittals have been properly marked. Refer to DOE O 475.2B, *Identifying Classified Information*, dated 10-3-14.

(c) Records of RD traffic must be maintained in accordance with DOE records and the National Archive and Records Administration General Records Schedule (GRS).

(4) A method of isolating the internal DOE network/NSN from the DOD SIPRNet, such as using a firewall, must be considered as a boundary protection service.

(5) Before RD is transmitted via NSN from an NNSA individual to a DOD recipient, the sender must verify the recipient has the appropriate final access authorization, such as the appropriate security clearance level, need-to-know, and access briefing (if applicable). The NNSA user must record and retain the verification data of the recipients.

f. Before RD is transmitted via NSN from an NNSA individual to a recipient external to NNSA/DOE, the sender must verify that the recipient has the appropriate final access authorization, such as a security clearance, need-to-know, and access briefing (if applicable). The NNSA user must record and retain the verification data of the recipients.

g. The individual sending the data must ensure that RD, to be transmitted via the NSN, has been reviewed for sensitivity, such as classification level and category, and appropriately marked in accordance with NNSA/DOE policies prior to transmission.

h. The AO must authorize the NSN controlled interface. Information systems that provide communication with or connectivity to the NSN may not connect to any other site network without the approval of the AOs for the NSN system(s) and site network.

THIS PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT F: INFORMATION CONDITION (INFOCON)

In addition to the requirements set forth in the Contractor Requirements Document (CRD), contractors are responsible for complying with Attachment F to this Policy. This Attachment provides more detailed information and requirements that are also applicable to federal employees.

1. INTRODUCTION. This attachment describes the minimum preparations and actions required to react uniformly to warnings of cybersecurity incidents, heighten or reduce the cyber-defensive posture, defend against computer network attacks, and mitigate sustained damage to National Nuclear Security Administration (NNSA) information and infrastructure, including computer and telecommunications networks and systems. The Information Condition (INFOCON) is a comprehensive defense posture and response based on the status of information systems, NNSA operations, and intelligence assessments of adversary capabilities and intent. The INFOCON system affects all personnel who use NNSA information systems, protects systems while supporting mission accomplishment, and coordinates the overall defensive effort through adherence to standards.

   The INFOCON system presents a structured, coordinated approach to react to adversarial attacks on NNSA information, computer systems, and networks and systems. While all systems are vulnerable to some degree, factors such as low-cost, readily available information technology, increased system connectivity, and remote access capability make computer network attack (CNA) an attractive option to an adversary. CNA is defined as "operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves." INFOCON also outlines countermeasures to scanning, probing, and other suspicious activity, unauthorized access, and data browsing. NNSA INFOCON measures focus on computer network-based protective measures due to the unique nature of CNA. Each level reflects a defensive posture based on the risk to NNSA operations through the disruption of information systems and networks.

2. CRITERIA AND PROCESSES.

   a. Each NNSA site's INFOCON response measure must be documented in the site's Cybersecurity Program Plan (CSPP) or the site's local INFOCON procedure.

   b. INFOCON procedures must be well integrated with the site's emergency procedures, incident-handling processes, and Continuity of Operations (COOP) plans.

   c. Cybersecurity incidents must be reported as described in Attachment D.

   d. Authorizing Officials (AOs) may evaluate their situation and recommend changes in the INFOCON to the NNSA Site Manager for sites under their cognizance. However, the INFOCON must remain at least as high as the current INFOCON level directed by NNSA. If the NNSA Site Manager agrees to the recommended change in INFOCON status, the AO must report the change to the Cyber Security

Program Manager (CSPM) and Chief Information Security Officer (CISO) within four hours.

e. The CSPM will notify the AO when the NNSA INFOCON level is changed, through the most rapid means available, and must notify the CSPM if recommended or directed INFOCON response measures conflict with organization or mission priorities within two hours of NNSA determination of INFOCON response measures.

f. The AO must disseminate INFOCON information within their respective organization and other organizations under their cognizance through the most efficient and rapid means available.

3. NNSA INFOCON. Assumptions have been made concerning the nature of CNA and computer network exploit (CNE) in development of the NNSA INFOCON system.

a. Shared Risk. In today's network-centric environment, risk assumed by one NNSA site is shared by all. Unlike most other security activities, a successful network intrusion in one NNSA location may, in many cases, facilitate access to other locations. This necessitates a common understanding of the situation and responses associated with the declared NNSA INFOCON level. These actions must be carried out concurrently at all NNSA locations for an effective defense posture.

b. Advance Preparation. Preparation is key, given the speed and reduced signature of CNA and CNE. Protective measures must be planned, prepared, practiced, and often executed well in advance of an attack. Preventive measures are emphasized in INFOCON responses because there may be little time to react effectively during the attack. Prevention of system compromise is preferable, but may not always be achievable.

c. Anonymity of Attacker. Attributing the attack to its ultimate source, if possible, will normally not occur until after the attack has been executed. This limits the range and type of options available to INFOCON decision makers. To effectively operate in this environment, knowledge of the adversary's identity cannot be a prerequisite to execution of defensive strategies and tactics.

d. Characterization of the Attack. Distinguishing between hacks, attacks, system anomalies, and operator error may be difficult. The most prudent approach is to assume malicious intent until an event is assessed otherwise.

e. INFOCON Levels. The NNSA INFOCON system presents a structured, coordinated approach to defend against and react to adversarial attacks on NNSA information, computer systems, and telecommunication networks and systems. The NNSA INFOCON system identifies the five levels of CNA and CNE conditions within NNSA.

Table 2-INFOCON Level Description from Highest To Lowest

INFOCON Level	Description
RED (Critical)	• Successful information system attack(s) detected that impact NNSA operations such as a Type 1 compromise or intrusion or Denial-of-Service (DoS), with a moderate or high impact. • Widespread incidents that undermine ability to function effectively. Significant risk of mission failure. • CNA against national infrastructure or National Security element.
ORANGE (Severe)	• Information system attack(s) detected with limited impact to NNSA operations. • Operating unit able to accomplish mission. • CNE that impacts NNSA operations such as a Type 1 compromise or intrusion or DoS, with low impact. • Nation- or Internet-wide CNE. • Intelligence indicates imminent attack against national infrastructure or national security element antibiotic. • Intelligence attack assessment(s) indicate a limited attack.
YELLOW (Elevated)	• Indications and Warnings (I&W) indicate targeting of specific system, location, unit, or operation. • Significant level of network probes, scans, or activities detected, indicating a pattern of concentrated reconnaissance. • Network penetration or DoS attempted with no impact to NNSA or Department of Energy (DOE) operations, such as a Type 2 attempted intrusion with a low impact. • Incident occurs at NNSA site that affects an NNSA Enterprise System, or it may impact another NNSA site, such as a Type 1 compromise or intrusion with a low impact. • Intelligence indicates imminent attack against NNSA or DOE site.
BLUE (Guarded)	• I&W indicate general threat. • Regional events occurring that affect U.S. interests and are likely to affect NNSA interests. May involve potential adversaries with suspected or known CNA capability. • Information system probes, scans, or other activities detected indicating a pattern of surveillance, such as a Type 2 reconnaissance activity with a moderate or high impact. • Nation- or Internet-wide computer network exploits, such as a Type 1 Website defacement, malicious code, or DoS, with low impact. • Increased or more predictable threat events. Incident occurs at NNSA or DOE site.
GREEN (Normal)	• No significant activity. Normal operations. • Network penetration or DoS attempted with no impact to NNSA, DOE, or site operations such as a Type 2 reconnaissance activity or intrusion attempts with a low impact. • Minimal attack success, successfully counteracted, such as a Type 1 unauthorized use with a low impact. • General threat unpredictable.

4. INFOCON ACTIVITIES.

a. Determining the INFOCON Level. There are three broad categories of factors that influence the INFOCON level: operational, technical, and intelligence, including foreign intelligence and law enforcement (LE) intelligence. Some factors may fall into more than one category. The INFOCON level is based on significant changes in one or more of these broad categories of factors. The decision to change the INFOCON level should be tempered by the overall operational and security context at that time. For example, an intruder could gain unauthorized access and not cause damage to systems or data. This may only warrant INFOCON BLUE or GREEN during peacetime, but it may warrant INFOCON ORANGE during a crisis. Also, the incident may warrant a high INFOCON level at the affected site, but not throughout NNSA as a whole.

b. Declaring the INFOCON Level. The NNSA CSPM recommends changes in the NNSA INFOCON level to the NNSA Chief Information Officer (CIO), who is responsible for declaring an NNSA INFOCON level. Assimilation and evaluation of information to assess the CNA and CNE situation NNSA-wide will be a collaborative effort coordinated by the CSPM.

c. Establishing the INFOCON Level. Managers of NNSA sites are responsible for assessing the situation and establishing the proper INFOCON level, based on evaluation of all relevant factors. NNSA Site Managers may change the INFOCON level of their organizations or site(s); however, they must remain at least as high as the current INFOCON level directed by NNSA. Managers changing the INFOCON level of their organization or site(s) must report to the CSPM.

d. Response Measures. Ideally, CNA/CNE operations will be based on advanced warning of an attack. Measures should be commensurate with the risk, the adversary's assessed capability and intent, and mission requirements. Over aggressive countermeasures may result in self-inflicted degradation of system performance and communication ability, which may contribute to the adversary's objectives. Managers must also consider what impact imposing a higher INFOCON level for their organization will have on connectivity with computer networks and systems of other NNSA sites and operations. Managers will notify the CSPM, through the cognizant Information System Security Manager (ISSM), if recommended or directed response measures conflict with organization or mission priorities. Regardless of the INFOCON level declared at the affected site, it is incumbent upon the affected site to report all unauthorized accesses in a timely manner, in accordance with the NNSA CSPP. Each NNSA site shall have documented procedures to guide their responses and ensure these procedures are well integrated with other site emergency procedures and COOP plans.

e. Reporting. Reporting of cybersecurity incidents must be accomplished as described in Attachment D. Note, however, that INFOCON levels assess potential or actual impact to NNSA operations and must be reported as follows:

(1) Reporting Channels. NNSA sites must report INFOCON level changes to the NNSA CSPM and the cognizant AO.

(2) Reporting Frequency. NNSA sites must report INFOCON level changes for their sites no later than four working hours after the INFOCON level has changed. Provide whatever information is available at the time and indicate information that is unknown or unavailable. Information missing from the initial report will be forwarded in a follow-up report within 24 hours of the initial report.

(3) Reporting Formats. Reports of changes in INFOCON level should be accompanied by an operational assessment of the situation, when appropriate. Report contents shall include, at a minimum:

(a) For all INFOCON Levels: Organization and location, date and time of report, current INFOCON level, reason for declaration of this INFOCON level, response actions taken, and point of contact (POC) information.

(b) INFOCON YELLOW and Higher: All of the above, plus U.S. Computer Emergency Response Team (CERT) or NNSA IARC Number (IARC will report to Center for Information Assurance and Cybersecurity (CIAC)) and Law Enforcement Agency (LEA) case number, with POC information, when available.

(c) INFOCON ORANGE and Higher: All of the above, plus system(s) affected, degree to which operational functions are affected, impact (actual or potential) on current and planned missions or general capabilities, restoration priorities, and workarounds.

f. Dissemination of NNSA INFOCON Level. The CSPM will notify the AO when the NNSA INFOCON level is changed, through the most rapid means available. The AO at the site must notify the CSPM, if recommended or directed INFOCON level response measures conflict with organizational or mission priorities, within two hours of NNSA determination of INFOCON level response measures. NNSA sites are responsible for rapid dissemination of the INFOCON level information within their organization, and to contractor organizations under their cognizance. Notification will include the following information:

(1) Date and time of report;

(2) Reason for declaration of this INFOCON level that includes a detailed description of the causal activities and type and system impact category;

(3) Current and planned operation(s) or capabilities, units or organizations, networks, systems, applications, or data assessed to be impacted or at risk;

(4) Recommended or NNSA-directed actions;

(5) References to relevant technical advisories and intelligence assessments;

(6) POC information; and

(7) Information that may assist sites in their response times.

5. RELATIONSHIP OF INFOCON LEVEL TO OTHER ALERT SYSTEMS. The INFOCON level may be changed based on the national or global situation, the intelligence community's level of concern, or other factors. Likewise, a change in INFOCON level may prompt a corresponding change in other alert systems.

6. EXERCISES. INFOCON procedures shall be practiced at all NNSA sites as part of their self-assessment programs to include operational impact assessments.

7. RECOMMENDED ACTIONS FOR INFOCON LEVELS.

Table 3-Recommended Actions for INFOCON Levels

LABEL (DESCRIPTION)	CRITERIA	RECOMMENDED ACTIONS
GREEN (Normal)	• No significant activity • Normal operations • General threat unpredictable • Network penetration or DoS attempted with no impact to NNSA, DOE, or site operations, such as a Type 2 reconnaissance activity or intrusion attempts with a low impact • Minimal attack success, successfully counteracted such as a Type 1 unauthorized use with a low impact	• Ensure all mission-critical information and information systems (including applications and databases) are identified • Ensure personnel receive Cybersecurity training annually • Ensure all points of access are identified, operationally necessary, and protected with Boundary Protection Services (BPS) • On a continuing basis, conduct normal cybersecurity practices • Refine and exercise preplanned protective measures • Review higher INFOCON level actions • Consider proactive execution of some, or all, higher INFOCON level actions

LABEL (DESCRIPTION)	CRITERIA	RECOMMENDED ACTIONS
BLUE (Guarded)	• I&W indicate general threat • Regional events occurring that affect U.S. interests and are likely to affect NNSA interests. May involve potential adversaries with suspected or known CNA capability. • Information system probes, scans, or other activities detected indicating a pattern of surveillance, such as a Type 2 reconnaissance activity, with moderate or high impact • Increased or more predictable threat events • Nation- or Internet-wide computer network exploits, such as a Type 1 Website defacement, malicious code, or DoS with low impact	Accomplish all actions at INFOCON GREEN, plus the following: • Execute appropriate cybersecurity practices to include closer monitoring of access points • Heighten user awareness • Execute appropriate defensive actions • Follow NNSA reporting procedures identified in NNSA cybersecurity policies • Review higher INFOCON level actions • Consider proactive execution of some, or all, higher INFOCON level actions • Review and update, as necessary, emergency response procedures

YELLOW (Elevated)	• I&W indicate targeting of specific system, location, unit, or operation
	• Significant level of network probes, scans, or activities detected indicating a pattern of concentrated reconnaissance
	• Network penetration or DoS attempted with no impact to NNSA or DOE operations, such as a Type 2 attempted intrusion with a low impact
	• Incident occurs at NNSA site that affects an NNSA enterprise system, or it may impact another NNSA site, such as a Type 1 compromise or intrusion with a low impact
	• Intelligence indicates imminent attack against NNSA or DOE site
		Accomplish all actions at INFOCON BLUE, plus the following:
		• Execute, as appropriate, the following cybersecurity practices:
		  ○ Enhance review of tools looking for anomalous behavior
		  ○ Increase frequency and strengthened reviews of auditing on critical systems
		  ○ Immediately review systems for security weaknesses and patch all critical systems, as needed
		• Isolate compromised systems immediately
		• Report suspected incursion or incidents early following NNSA reporting procedures
		• Assess planned responses in light of the precise characteristics of the threat as seen and refine planned responses, as necessary
		• Check communications with designated emergency response or command locations
		• Review higher INFOCON level actions
		• Consider proactive execution of some, or all, higher INFOCON level actions

LABEL (DESCRIPTION)	CRITERIA	RECOMMENDED ACTIONS

ORANGE (Severe)	• Information system attack(s) detected with limited impact to NNSA operations
	• Operating unit able to accomplish mission
	• CNE that impacts NNSA operations, such as a Type 1 compromise or intrusion or DoS with low impact.
	• Nation- or Internet-wide CNE
	• Intelligence indicates imminent attack against national infrastructure or national security element
	• Intelligence attack assessment(s) indicate a limited attack
		Accomplish all actions at INFOCON YELLOW, plus the following:
		• Execute, as appropriate, the following cybersecurity practices:
		  ○ Increase frequency and strengthened reviews of auditing on critical systems
		  ○ Reconfigure BPS (e.g., firewalls, routers, and Intrusion Prevention Systems (IPSs)) to limit external connections and traffic to absolute minimum need for current mission operations
		  ○ Reconfigure systems to minimize access points and increase security
		  ○ Minimize traffic enclaves to absolute minimum needed for current mission operations
		  ○ Consider eliminating Internet access to/from all non-mission-critical systems and networks
		• Isolate any compromised systems immediately
		• Follow NNSA reporting procedures

RED (Critical)	• Successful information system attack(s) detected that impact NNSA operations, such as a Type 1 compromise and/or intrusion or DoS with a moderate or high impact
	• Widespread incidents that undermine ability to function effectively
	• Significant risk of mission failure
	• Computer Network Attack against national infrastructure or national security element
		Accomplish all actions at INFOCON ORANGE, plus the following:
		• Execute, as appropriate, the following cybersecurity practices:
		  ○ Reconfigure information systems and networks to use BPS-controlled connections and traffic
		  ○ Execute procedures for ensuring graceful degradation of information systems and network(s)
		  ○ Disconnect all non-mission-critical systems and networks from Internet
		  ○ Implement procedures for stand-alone or manual operations
		• Follow NNSA reporting procedures
		• Execute applicable portions of COOP plans

8. FACTORS INFLUENCING INFOCON. When determining the appropriate defensive posture, many factors must be considered. This appendix lists several factors that managers should consider when determining the INFOCON. Note that this list is offered as broad guidance. Other factors may also be considered.

   a. Other I&W (including domestic threats). NSA IPC Alerts, National Infrastructure Protection Center (NIPC) advisories, threats, warnings, and LEA intrusion reports.

   b. CNA intelligence assessments.

   c. Current world situation. Increased tensions with a nation possessing CNA capability may precede CNA operations against us.

   d. Other alert systems. Managers must determine if a change in one alert status will cause a corresponding change in another alert status.

   e. Dependence of NNSA functions upon particular information systems. This type of analysis may suggest the degree to which a particular network, system, application, or database is mission-critical.

   f. Manager's assessment of mission-critical information system readiness. This readiness may be determined from the networks' security posture, vulnerability, extent of compromise, etc.

   g. Manager's assessment of readiness to coordinate the protection of critical infrastructure and key resources identified under Homeland Security Presidential Directive-7 (HSPD-7), *Critical Infrastructure Identification, Prioritization, and Protection.*

   h. Incident reports. These are roughly analogous to attack assessments.

   i. Trend analyses. Reports showing number, type, and frequency of attacks, systems targeted, and hot Internet Protocol (IP) addresses.

   j. Technical impact assessment. This information may be included in an incident report or may result from follow-on analysis. This assessment may include the extent of system compromise or disruption and the degree to which system confidentiality, integrity, availability, and authentication have been affected.

   k. Operational impact assessment. A key element in determining the INFOCON. The process for assessing operational impact also lays the groundwork for executing preventive measures, developing workarounds, and establishing restoration priorities.

   l. ISSM's assessment of the potential for an information attack. Although much objective data is available on which to base the decision, the final judgment for declaring an INFOCON level change rests with the AO. Objective assessment of

the situation and prudent analysis of all available information must be integrated with the manager's experience and leadership to determine the organization's appropriate defensive posture.

APPENDIX 1: DEFINITIONS

a. Authority to Operate (ATO) – The official management decision given by a senior organizational official or CISO to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

b. Authorizing Official (AO) – A senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations and assets, individuals, other organizations, and the Nation. The Enterprise AO is appointed by the CIO.

c. Binding Operational Directive (BOD) – Under the *Federal Information Security Modernization Act* (FISMA) of 2014, DHS is provided with the authority to administer the implementation of federal cybersecurity policies. In order to carry out this important responsibility, DHS is authorized by Congress to issue binding operational directives, policies that direct agencies to monitor cybersecurity.

d. Center on National Security Systems (CNSS) – The CNSS provides a forum for the discussion of policy issues and is responsible for setting national-level Information Assurance policies, directives, instructions, operational procedures, guidance, and advisories for U.S. Government (USG) departments and agencies for the security of National Security Systems (NSS) through the CNSS Issuance System. The CNSS is directed to ensure the security of NSS against technical exploitation by providing: reliable and continuing assessments of threats and vulnerabilities and implementation of effective countermeasures; a technical base within the USG to achieve this security; and support from the private sector to enhance that technical base ensuring that information systems security products are available to secure NSS.

e. Chief Information Security Officer (CISO) – Senior Agency Information Security Officer with information system or security management/oversight responsibilities.

f. Contractor Assurance System (CAS) – Requirements for a contractor assurance system are described in DOE O 226.1B, *Implementation of Department of Energy Oversight Policy*, Attachment 1, Appendix A "Contractor Assurance Systems."

g. Cybersecurity – The ability to protect or defend the use of cyberspace from attacks (CNSSI 4009).

h. Cybersecurity Improvement Plan (CSIP) – A plan that describes items that have been identified as representing some degree of risk or that require some type of corrective action.

i. Cybersecurity Program (CSP) – A program established to provide 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).

j. Cybersecurity Program Plan (CSPP) – The CSPP is the document that outlines the policies, procedures, and practices of an element's cybersecurity program. The CSPP is a management-level document and details the organization's policies, procedures, and practices for ensuring effective cybersecurity. It also explains the site or application-specific environment, missions, and threats. The policies, procedures, practices, environments, missions, and threats for major applications are also documented in a CSPP.

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

l. Enterprise, Governance, Risk, and Compliance (EGRC) – The EGRC is the official corporate and enterprise program repository that will be used to conduct continuous performance monitoring and reporting of information security program management, operations, and technical controls (i.e., Authority to Operate (ATO) packages, deviations, incident management reporting).

m. Enterprise System – Systems within NNSA where the authorization boundary covers multiple sites and multiple local Authorization Official jurisdictions.

n. Information Assurance Response Center (IARC) – NNSA's Information Assurance Response Center located in Las Vegas, NV, that continuously monitors all activity going through the nuclear security enterprise computer firewall system, providing intrusion detection and event forensics for the NNSA enterprise.

o. Information Condition (INFOCON) – A comprehensive defense posture and response based on the status of information systems, NNSA operations, and intelligence assessments of adversary capabilities and intent. The INFOCON system affects all personnel who use NNSA information systems, protects systems while supporting mission accomplishment, and coordinates the overall defensive effort through adherence to standards.

p. Information Management Governance Board (IMGB) – The DOE Information Management Governance Board (IMGB) serves as a forum for collaboration, development, coordination, and execution of efforts relating to DOE enterprise cyber activities and issues.

q. Information System Security Manager (ISSM) −An employee appointed by the CISO who must have a working knowledge of system functions and cybersecurity policies and protection measures, and manages federal systems.

r. Information System Security Officer (ISSO) – An individual responsible for ensuring that the appropriate operational security posture is maintained for an information system and, as such, works in close collaboration with the information system owner.

s. Information System Security Plan (ISSP) – A plan that includes a description of the controlled interface technical and procedural agreements required for transmission, including clearance and briefings required for access to specific classification levels and categories of information, between the NNSA system and NNSA Secret Network (NSN).

t. Joint Cybersecurity Coordination Center (JC3) – JC3 is managed and operated by DOE CIO. JC3 provides DOE with incident response, reporting, tracking, and other computer security support to collect, analyze, and share cybersecurity information and to serve as the DOE incident response coordination and reporting element from across the DOE 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.

u. Plans of Action and Milestones (POA&M) – a management tool for tracking the remedial action and mitigation of cybersecurity program and system level findings and weaknesses.

v. Protected Distribution System (PDS) – Wireline or fiber-optic distribution systems used to transmit unencrypted classified National Security Information through an area of lesser classification or control.

w. Restricted Data -- All data concerning the design, manufacture, or use of nuclear weapons; production of special nuclear material; or use of special nuclear material in the production of energy except for data declassified or removed from the RD category pursuant to section 142 of the *Atomic Energy Act*.

x. SIGMA -- The "Sigma categories" are subsets of nuclear weapons information classified under the *Atomic Energy Act* that are grouped by subject matter. For more information on SIGMA, please see DOE O 452.8, *Control of Nuclear Weapon Data*.

y. Site Risk Management Council (SRMC) – Site-level council responsible for managing information management risks at their respective sites. The council is established to serve as the common risk management resource for stakeholders having a vested interest in the mission success of the site. Additionally, these councils support the federal appointed AOs, who are the risk approving and

accepting authorities at their respective sites, to manage the risks associated with information systems operated within their area of responsibility.

z. TEMPEST – A name referring to the investigation, study, and control of compromising emanations from telecommunications and automated information systems equipment.

APPENDIX 2: REFERENCES

a. Federal Laws and Regulations:

(1) 44 U.S.C. § 3541 et seq., *Federal Information Security Management Act* of 2002 (FISMA), enacted December 2002.

(2) 32 CFR 2002, *Controlled Unclassified Information*, dated 9-14-2016.

(3) 32 CFR 2001.23, *Classification Marking in the Electronic Environment*, dated 7-01-10.

(4) 32 CFR 2001.24, *Additional Requirements*, dated 6-28-10.

(5) E.O. 13526, *Classified National Security Information*, dated 12-29-09.

(6) E.O 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, dated 10-7-11.

b. National Security Directive 42, National Policy for the Security of National Security Telecommunications and Information Systems, July 5, 1990.

c. Office of Management and Budget (OMB) Circulars. Located at https://omb/circulars_default.

d. OMB Memoranda Pertaining to Information Technology Security and Management. Located at https://obamawhitehouse.archives.gov/omb/memoranda_default.

e. Department of Homeland Security (DHS), Binding Operational Directive, BOD-15-01, Critical Vulnerability Mitigation Requirement For Federal Civilian Executive Branch Departments' and Agencies' Internet-Accessible Systems, dated 5-21-2015.

Note: By the authority from Congress in the *Federal Information Security Modernization Act* of 2014, the Secretary of Homeland Security is responsible for issuing Binding Operational Directives. These Directives require agencies to mitigate risks to their information systems based on DHS guidance.

f. DOE Orders, Manuals, Notices, and Guidelines. Located at https://www.directives.doe.gov/directives.

(1) DOE O 471.6 Change 2, *Information Security*, dated 5-15-15.

(2) DOE O 475.1, *Counterintelligence Program*, dated 12-10-04.

(3) DOE O 415.1, *Information Technology Project Management*, dated 12-03-12.

(4) DOE O 470.6, *Technical Security Program*, dated 9-2-15.

(5) DOE O 226.1B, *Implementation of Department of Energy Oversight Policy*, dated 4-25-11.

(6) DOE O 205.1B Change 3, *Department of Energy Cybersecurity Program*, dated 9-21-14.

(7) DOE O 206.1, *Department of Energy Privacy Program*, dated 1-16-09.

g. NNSA Policies:

(1) SD 470.4-1, *Defense Nuclear Security Federal Oversight Process*, dated 4-1-16.

(2) SD 226.1B, *NNSA Site Governance*, dated 8-12-16.

(3) BOP-00.01A, *Senior Leadership Councils*, dated 1-22-15.

h. Other:

(1) NSPD-28, *United States Nuclear Weapons Command and Control, Safety, and Security*, dated 6-20-03.

(2) National Security Agency/Central Security Service, NSA/CSS Policy Manual 9-12, *Storage Device Sanitization Manual* , dated 12-15-14.

(3) Issuances of the Committee on National Security Systems (CNSS). Index of National Security Systems' Issuances can be found at https://www.cnss.gov/CNSS/issuances/Issuances.cfm.

(4) National Institute of Standards and Technology (NIST) Standards and Guidelines. Directory of NIST Standards and Guidelines can be found at http://csrc.nist.gov/publications/.

(5) Federal guidance on implementing secure configuration for NSS and unclassified systems is at http://web.nvd.nist.gov/view/ncp/repository.

(6) Community Gold Standard (CGS) for NSS is at https://www.iad.gov/iad/library/ia-guidance/ia-standards/cgs/index.cfm.

(7) NIST Computer Resource Center, *National Supply Chain Risk Management Practices for Federal Information Systems* (NISTIR) 7622, dated 10-16-12.

(8) Committee in National Security Systems (CNSS) Instruction 7000, *TEMPEST Countermeasures for Facilities*, May 2004.

(9) CNSS 5000, *TEMPEST Fundamentals*, February 1982.

(10) DOD 8570.01, Information Assurance Workforce Improvement Program, 11-10-2015 http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf.

(11) Delegation Order No. 003.03-02, *Delegation of Authority− Cyber Security*, dated 2-16-11.