

Approved: 05-20-2024

**SUBJECT: SECURITY AND USE CONTROL OF NUCLEAR EXPLOSIVES AND
NUCLEAR WEAPONS**

1. PURPOSE. This Department of Energy (DOE) Order establishes the nuclear explosive security, use control (UC), and Nuclear Enterprise Assurance (NEA) requirements to implement DOE O 452.1, *Nuclear Explosive and Weapon Surety (NEWS) Program*, current version, to ensure authorized use of nuclear weapons, when directed by proper authority, and protect against deliberate unauthorized acts, deliberate unauthorized use (DUU), and denial of authorized use (DAU).
2. CANCELLATION. DOE O 452.4C, *Security and Use Control of Nuclear Explosives and Nuclear Weapons*, dated 8-28-2015. Cancellation of a directive does not, by itself, modify or otherwise affect any contractual or regulatory obligation to comply with the directive. Contractor Requirements Documents (CRDs) that have been incorporated into a contract remain in effect throughout the term of the contract unless and until the contract or regulatory commitment is modified to either eliminate requirements that are no longer applicable or substitute a new set of requirements.
3. APPLICABILITY.
 - a. Departmental Applicability. This Order applies to all Departmental elements that are involved in maintaining and enhancing the safety, security, reliability, and performance of the United States nuclear weapons stockpile, including the ability to design, produce, test, and certify weapons that meet national security and NEWS program requirements.
 - b. The Administrator will ensure that National Nuclear Security Administration (NNSA) employees and contractors comply with their respective responsibilities under this Order. Nothing in this Order will be construed to interfere with the NNSA Administrator's authority under section 3212(d) of Public Law (P.L.) 106-65 to establish Administration specific policies, unless disapproved by the Secretary.
 - c. DOE Contractors. The CRD, Attachment 1, sets forth requirements of this Order that must apply to contracts that include the CRD. The CRD must be included in all contracts involved in maintaining and enhancing the safety, reliability, and performance of the United States nuclear weapons stockpile. Attachments 2 and 3 provide definitions and references, respectively, used in this order.

- d. Equivalencies and Exemptions for DOE O 452.4D. Equivalencies and exemptions from the requirements of this Order are processed in accordance with DOE O 251.1, *Departmental Directive Program*, current version. Requests must be sent to the NNSA Office of Stockpile Management, Defense Programs.
- (1) Exemptions. None.
 - (2) Equivalency. In accordance with the responsibilities and authorities assigned by Executive Order 12344, codified at Title 50 United States Code (U.S.C.) sections 2406 and 2511 and to ensure consistency throughout the joint Navy/DOE Naval Nuclear Propulsion Program, the Deputy Administrator for Naval Reactors (Director) will implement and oversee requirements and practices pertaining to this Directive for activities under the Director's cognizance, as deemed appropriate.
4. REQUIREMENTS. Nuclear explosives and nuclear explosive operations (NEOs) require safety, security, UC, and assurance considerations due to the potentially unacceptable consequences of an accident, unauthorized acts, or adversarial subversion attempts. Contextually, this Order primarily addresses malevolent, unauthorized acts.

Nuclear Explosive Surety Standards prescribed in DOE O 452.1, current version, strongly emphasize integrating best practices to ensure that NEOs are used only by an authorized and directed by proper authority; and the assurance that design and performance of NEOs will prevent unintended/unauthorized nuclear detonation, unintended main charge High Explosive Violent Reaction (HEVR), and the subversion of weapon functionality. These goals contribute to the overarching objective to reduce the likelihood of specified consequences to as low as reasonably practicable. Notify NNSA's Office of Stockpile Management of any conflicts between the following requirements and those prescribed in other DOE or NNSA directives.

- a. Nuclear Explosives Security and Use Control. Consistent with Nuclear Explosive Surety Standards and NEWS Program objectives prescribed in DOE O 452.1, current version, DOE/NNSA must:
- (1) Protect nuclear explosives and nuclear weapons by including a combination of administrative, procedural, and technical measures designed to ensure authorized use when directed by proper authority and protect against deliberate unauthorized acts, DUU, and DAU.
 - (2) Establish complementary programs/subprograms focused on nuclear explosive and weapon security, UC, and digital assurance that are comprised of an integrated system composed of design; review; installation; and production of features, devices, and other measures to maintain control of nuclear explosives and nuclear weapons at all times throughout their life cycle.

- (3) Ensure nuclear explosives and weapon security, as well as UC programs and digital assurance, include the following major elements:
 - (a) Function and operation of UC features, devices, and other security measures that are in conformity with policies, responsibilities, and procedures set forth in DOE 452- and 470- series Orders.
 - (b) Assessment of security and UC measures for nuclear explosives and nuclear weapons, including design features that are incorporated and functional at the earliest possible point during assembly and removed at the latest possible point during disassembly or dismantlement.
 - (c) Evaluation of security and UC upgrades to be implemented during weapon retrofit, alteration, or refurbishment for all nuclear weapons to meet current nuclear surety requirements.
 - (d) Assessment of design attributes that may include a combination of administrative and technical measures, and digital assurances that are designed to prevent or delay DUU of nuclear explosives and nuclear weapons.
 - (e) Human Reliability Program (HRP) as required by Title 10 Code of Federal Regulations (CFR) Part 712, to ensure the reliability of DOE and contractor employees who require access to designated components, nuclear explosives, or nuclear weapons.
 - (f) Measures to prevent deliberate unauthorized acts, from degrading the effectiveness of UC measures incorporated in or used for nuclear explosives or nuclear weapons.
 - (g) Measures to prevent or delay DUU, deliberate unauthorized acts, DAU, or loss of control during planned NEOs.
 - (h) Measures to assist the recapture and recovery of lost or stolen nuclear explosives or nuclear weapons.
 - (i) Stockpile surveillance to ensure that UC devices and components meet specified requirements and have not been altered.
 - (j) Deliberate unauthorized act, DUU, and DAU evaluations performed periodically and documented that may be specific to a DOE nuclear weapon, nuclear explosive, NEO, class of operations, facility, or site (see also paragraph 4.c.).
 - (k) Measures that must be periodically assessed against existing and emerging threats as well as technological opportunities for improvement.

- (l) Security of the supply chain and protection against components and assemblies with malicious content that could override or degrade UC or nuclear weapons functionality.
 - (m) Measures to ensure cyber security in all aspects of design, sourcing and coding, procurement, production, and sustainment to ensure that critical program information and systems are secure.
 - (n) Necessary measures for interagency information sharing and cooperation in threat identification, supplier vetting, and risk mitigation.
 - (o) Assessments that weapons systems, including associated systems and components/codes, have not been subverted or corrupted.
 - (p) Records maintenance in accordance with National Archives and Records Administration-approved DOE or site-specific records retention schedules.
 - (q) Research and Development (R&D) to protect against deliberate unauthorized acts, DUU, and DAU of nuclear explosives and nuclear weapons. Reference paragraph 4.e for required R&D program elements.
- (4) Coordinate protection measures and program elements related to nuclear weapon design for consistency with DoD operational requirements.
- (5) Incorporate integrated risk management to ensure controls implemented to support the Nuclear Explosive Surety Standards for one aspect of surety (i.e., safety, security, UC, or digital assurance) are evaluated for adverse impact(s) on the other surety aspects.
- b. Nuclear Enterprise Assurance (NEA). NEA is an NSE countersubversion program established to detect and prevent subversion and mitigate the consequences of discovered subversions affecting nuclear weapons throughout their entire lifecycle, as well as to nuclear weapons enabling capabilities. NEA supports surety for Nuclear Explosives and Weapons, including providing assurance that components/systems are not subverted or compromised during design and production, in support of preventing deliberate unauthorized acts that may lead to DAU, or degradation of weapon reliability and/or performance. NEA increases system assurance for nuclear weapons and enabling capabilities, including digital assurance. DOE/NNSA must protect against adversarial subversion of the NSE supply chain; and evaluate documented evidentiary information that provides assurance that nuclear weapons and nuclear weapon-enabling capabilities have not been subverted. Reference NNSA Supplemental Directive (NNSA SD) 452.4-1, *Nuclear Enterprise Assurance*, current version, for detailed NEA requirements and NEA Steering Group (NEASG) responsibilities.

- c. Deliberate unauthorized act, DUU, and DAU evaluations.
 - (1) Conduct evaluations for DOE/NNSA nuclear explosives, digital controls/codes, nuclear weapons, NEOs, and certain non-NEO production activities, assessing controls as they apply to the critical component, nuclear explosive, or nuclear weapons against credible existing and emerging threats and technological advancements to determine the adequacy of the controls. Reference NNSA SD 452.4, *Implementation and Evaluation of Controls to Prevent Deliberate Unauthorized Use*, current version, for additional direction for the evaluations.
 - (2) Evaluations must meet the following criteria:
 - (a) NNSA Sites with NEOs. The deliberate unauthorized act, DUU, and DAU evaluations will address NEO processes, testers, tooling, and facilities to ensure that controls are adequate to meet the UC elements of DOE O 452.1, current version, Nuclear Explosive Surety Standards applicable to NEOs.
 - (b) NNSA Sites without NEOs. The deliberate unauthorized act, DUU, and DAU evaluations will address DOE weapon component designs, testers, and subsystem/component production to ensure the integrity of product used in nuclear explosives and nuclear weapons is adequate to not jeopardize conformance with the UC elements of DOE O 452.1, current version, Nuclear Explosive Surety Standards.
- d. Joint DOE/NNSA and DoD Collaboration.
 - (1) DOE/NNSA must cooperate with DoD as required to provide protection against deliberate unauthorized acts, DUU and DAU, and to assess the effectiveness of surety features for all U.S. nuclear weapon systems throughout their life cycles. These features must be consistent with DoD operational requirements and must continually be assessed against existing and emerging threats as well as technological opportunities for improvement.
 - (2) DOE/NNSA must assist DoD in designating nuclear command and control critical equipment and components to ensure that these items are developed and maintained to meet the criteria designated in National Security Directives and the Nuclear Explosive and Weapon Surety (NEWS) and UC programs.
- e. Research and Development (R&D).
 - (1) Provide resources and conduct R&D for security, digital assurance, and UC measures that protects against deliberate unauthorized acts, DUU, and DAU of nuclear explosives and nuclear weapons, consistent with Nuclear

Explosive Surety Standards and NEWS Program objectives prescribed in DOE O 452.1, current version.

- (2) Recommendations from these R&D activities are provided for use by project managers, project teams, project officer groups, and decision-makers within DOE/NNSA. The objective of such improvements is to minimize the overall risk of deliberate unauthorized use (DUU) and denial of authorized use (DAU) by providing an effective adversary delay or denial capability for the overall nuclear weapon system that either is inherent in the design or does not require human intervention. Specifically, security and UC R&D must:
 - (a) Pursue technologies that can enhance security and UC for new and existing systems.
 - (b) Develop nuclear weapon measures to provide assurance of operation as designed when authorized for use.
 - (c) Design nuclear weapon features that enhance secure critical command and control communications.
 - (d) Develop technologies to aid in the recapture and recovery of weapons.
 - (e) Develop approaches to efficiently detect subversion.
 - (f) Ensure personnel responsible for R&D of security, UC, and NEA features appropriately protect as classified and controlled unclassified information (according to sensitivities) the improvements and information related to newly developed security, UC, and NEA measures.

5. RESPONSIBILITIES. See NNSA SD 452.4-1 for full NEA-related NNSA responsibilities.

- a. Director, Office of Intelligence and Counterintelligence (DOE/IN).
 - (1) Provides intelligence and counterintelligence support for nuclear weapon security, UC, and NEA activities as requested by NNSA.
 - (2) Serves as a member of the NEASG.
- b. Associate Administrator for Counterterrorism and Counterproliferation (NA-80). Establishes programs for coordinating and assisting in the recapture and recovery of U.S. nuclear explosives or nuclear weapons for which physical control has been lost.

- c. Associate Administrator for Infrastructure (NA-90).
 - (1) Develops and implements programs, policies, processes, and procedures to enable safe operations, ensure effective infrastructure, and integrate or implement activities and programs across the NNSA Nuclear Security Enterprise.
 - (2) Advises the Assistant Deputy Administrator for Stockpile Management (NA-12) on safe operations and infrastructure requirements to implement elements of the Nuclear Explosive Surety Standards prescribed in DOE O 452.1, current version.
- d. Associate Administrator and Chief for Defense Nuclear Security (NA-70).
 - (1) Serves as the DOE Officially Designated Federal Security Official responsible for the development and implementation of security programs, operations, and facilities under the purview of NNSA, including physical security, personnel security, materials control and accountability, classified and controlled unclassified information protection, and technical security.
 - (2) Advises the Assistant Deputy Administrator for Stockpile Management (NA-12) on safeguards and security requirements to implement elements of the Nuclear Explosive Surety Standards prescribed in DOE O 452.1, current version.
 - (3) Establishes programs for coordinating and assisting in the recapture and recovery of U.S. nuclear explosives or nuclear weapons for which physical control has been lost.
- e. Associate Administrator for Information Management and Chief Information Officer (NA-IM). Provides cyber asset support to the Office of Defense Programs (NA-10) for nuclear weapon security, UC, and NEA activities.
- f. Assistant Deputy Administrator for Stockpile Management (NA-12).
 - (1) Oversees the management and integration of all aspects of nuclear explosives and weapon security, UC, and NEA programs or activities, except for R&D.
 - (2) Represents the Office of Defense Programs (NA-10) in coordinating and assisting DoD and other non-DOE entities in the recapture and recovery of U.S. nuclear explosives or nuclear weapons for which physical control has been lost.
 - (3) Represents DOE/NNSA regarding U.S. nuclear weapons and nuclear weapons systems UC to DoD and other non-DOE entities.

- (4) Ensures active and continuous review of the nuclear stockpile is being conducted to identify Program concerns and ensures implementation of stockpile improvement or controls to address identified concerns.
- (5) Directs assessment of the effectiveness of UC features of U.S. nuclear weapons in DOE and DoD custody.
- (6) Approves designated components for Defense Programs (NA-10) as referenced in subparagraphs 4.a.(3)(a) and 4.d.(2).
- (7) Establishes and oversees the Nuclear Enterprise Assurance activities to effectively address the “ensure authorized use” mission area of UC and to preclude denial of authorized use, collaborates with DoD and other non-DOE entities on such matters.
- (8) Charters and leads the NEASG, to include approving steering group membership and serving as the final decision-making authority for issues when steering group members cannot reach consensus.
- (9) Assists DoD and other non-DOE entities in designating nuclear command and control critical equipment and ensuring that it is developed to meet criteria specified in National Security Directives.
- (10) Ensures collaboration between the Office of Stockpile Management (NA-12), Office of Research, Development, Test & Evaluation (NA-11), Office of Systems Engineering and Integration (NA-18), and Office of Production Modernization (NA-19) to establish programs to incorporate improved UC measures in the stockpile and promote those programs found to be cost effective and feasible.
- (11) Manages periodic deliberate unauthorized act, DUU, and DAU assessments of nuclear explosives and nuclear weapons to evaluate and document existing and emerging threats and technological advancements associated with deliberate unauthorized acts, DUU, and DAU.
- (12) Accepts risk for the Office of the Deputy Administrator for Defense Programs throughout product realization life cycle for stockpile systems, life extension programs, alterations, including those identified by NEA activities.

g. Assistant Deputy Administrator for Secure Transportation (NA-15).

- (1) Ensures active and continuous review of the aspects of nuclear explosives and weapon security, and UC under his/her purview is conducted to identify program concerns and to ensure implementation of improvement or controls to address identified concerns.

- (2) Assesses the effectiveness of the integrated system of controls to protect nuclear explosives and nuclear weapons under his/her cognizance against deliberate unauthorized acts.
 - (3) Periodically evaluates and documents existing and emerging threats and technological advancements associated with deliberate unauthorized acts.
- h. Assistant Deputy Administrator for Research, Development, Test & Evaluation (NA-11).
 - (1) Manages the R&D aspects of nuclear explosives and weapon security, UC, and NEA activities.
 - (2) Manages R&D efforts on a broad range of surety methods, devices, and technologies to significantly improve the security and UC of nuclear weapons and nuclear weapon systems, and to protect, detect, and mitigate subversion of nuclear weapons and nuclear weapon enabling capabilities.
 - (3) Coordinates with Assistant Deputy Administrator for Stockpile Management (NA-12) and establishes security and UC priorities for R&D efforts, resources, and designates critical components for UC development.
 - (4) Allocates R&D resources and pursues:
 - (a) Technologies that can enhance security and UC for new and existing systems.
 - (b) Nuclear weapon measures to provide assurance of operation as designed when authorized for use.
 - (c) R&D of controls to prevent deliberate unauthorized acts, DUU, and DAU of nuclear explosives and nuclear weapons.
 - (5) Works with the Office of Stockpile Management (NA-12) to establish programs to incorporate improved UC measures in the stockpile.
- i. Director, Office of Stockpile Production Integration (NA-121).
 - (1) Establishes and maintains Directives to govern NEA implementation.
 - (2) Ensures NEA requirements are applied to all nuclear weapon programs throughout the respective nuclear weapon's life cycle, including protection of nuclear weapon-enabling capabilities and cross-cutting functions.
 - (3) Establishes and maintains intelligence information and communication processes/protocols to facilitate NNSA and DOE/IN collaboration to effectively implement NEA requirements.

- (4) Develops and implements processes/protocols for interagency and NSE information sharing and cooperation regarding threat identification, supplier vetting, and risk mitigation.
- (5) Establishes a review and decision-making steering group for NEA activities comprised of senior Federal officials from NNSA and DOE Headquarters, including Intelligence and Counterintelligence (DOE/IN), and others as approved by the ADA for Stockpile Management (NA-12).
- (6) Recommends offices for membership in the NEA steering group to the ADA for Stockpile Management (NA-12).

j. NNSA Field Office Managers.

- (1) Ensure implementation of nuclear explosives and weapon security, UC, and NEA programs and activities where applicable.
- (2) Conduct audits (based on competent, independent reviews) that ensure each NEO authorized meets the use control elements of DOE O 452.1, current version, Nuclear Explosive Surety Standards applicable to NEOs. Retain documentation of these reviews, their conclusions, and resolution of findings. If a Field Office lacks qualified subject matter experts to perform the review, assistance may be requested from the Office of Stockpile Management.
- (3) Conduct audits (based on competent, independent reviews) that ensure deliberate unauthorized act, DUU, and DAU reviews for non-NEO production does not jeopardize conformance with UC elements of the DOE O 452.1, current version, Nuclear Explosive Surety Standards. Retain documentation of these reviews, their conclusions, and resolution of findings. If a Field Office lacks qualified subject matter experts to perform the review, assistance may be requested from the Office of Stockpile Management.
- (4) Notify contracting officers which contracts are affected by the CRD to this Order.

k. Contracting Officers. Once notified, incorporate the CRD and applicable attachments of this Order into each affected contract.

- 6. INVOKED STANDARDS. This Order does not invoke any DOE technical standards or industry standards as required methods. Any technical standard or industry standard that is mentioned in or referenced by this Order is not invoked by this Order. Note: DOE O 251.1D, Appendix J, provides a definition for invoked technical standards.
- 7. DEFINITIONS. See Attachment 2.
- 8. REFERENCES. See Attachment 3.

9. CONTACT. Questions concerning this Order should be addressed to the Assistant Deputy Administrator for Stockpile Management, 202-586-4879.

BY ORDER OF THE SECRETARY OF ENERGY:



DAVID M. TURK
Deputy Secretary

ATTACHMENT 1
CONTRACTOR REQUIREMENTS DOCUMENT
DOE O 452.4D, *Security and Use Control of Nuclear Explosives and Nuclear Weapons*

This Contractor Requirements Document (CRD) establishes the requirements for Department of Energy (DOE) contractors, including National Nuclear Security Administration (NNSA) contractors, whose contracts involve maintaining and enhancing the safety, reliability, and performance of the United States nuclear weapons stockpile, including the ability to design, produce, and test to meet national security and Nuclear Explosive and Weapon Surety (NEWS) program requirements.

Regardless of the performer of the work, the contractor is responsible for compliance with the requirements of this CRD and the attachments to this Order. Attachments 2 and 3 provide definitions and references, respectively, used in this order. The contractor is responsible for flowing down the requirements of this CRD and applicable attachments to subcontractors at any tier to the extent necessary to ensure the contractor's compliance with the requirements.

1. Nuclear explosives and nuclear explosive operations (NEOs) require safety, security, UC, and assurance considerations due to the potentially unacceptable consequences of an accident, unauthorized acts, or adversarial subversion attempts. Contextually, this Order primarily addresses malevolent, unauthorized acts.
2. Nuclear Explosive Surety Standards prescribed in DOE O 452.1, current version, strongly emphasize integrating best practices to ensure that NEOs are used only by an authorized and directed by proper authority; and the assurance that design and performance of NEOs will prevent unintended/unauthorized nuclear detonation, unintended main charge High Explosive Violent Reaction (HEVR), and the subversion of weapon functionality. These goals contribute to the overarching objective to reduce the likelihood of specified consequences to as low as reasonably practicable. Notify NNSA's Office of Stockpile Management of any conflicts between the following requirements and those prescribed in other DOE or NNSA directives.
 - a. Nuclear Explosives Security and Use Control. Consistent with Nuclear Explosive Surety Standards and NEWS Program objectives prescribed in DOE O 452.1, current version, contractors must:
 - (1) Protect nuclear explosives and nuclear weapons by including a combination of administrative, process, and technical measures designed to ensure authorized use when directed by proper authority and protect against deliberate unauthorized acts, DUU, and DAU.
 - (2) Establish complementary programs/subprograms focused on nuclear explosive and weapon security, UC, and digital assurance that are comprised of an integrated system composed of design; review; installation; and production of features, devices, and other measures to

maintain control of nuclear explosives and nuclear weapons at all times throughout their life cycle.

- (3) Ensure nuclear explosives and weapon security, as well as UC programs and digital assurance, include the following major elements:
 - (a) Function and operation of UC features, devices, and other measures that are integrated with security measures referenced in DOE O 452- and 470- series Orders to maximize system effectiveness and manage cost.
 - (b) Assessment of security and UC measures for nuclear explosives and nuclear weapons, including design features that are incorporated and functional at the earliest possible point during assembly and removed at the latest possible point during disassembly or dismantlement.
 - (c) Evaluation of security and UC upgrades to be implemented during weapon retrofit, alteration, or refurbishment for all nuclear weapons to meet current nuclear surety requirements.
 - (d) Assessment of design attributes that may include a combination of administrative and technical measures, and digital assurances that are designed to prevent or delay DUU of nuclear explosives and nuclear weapons.
 - (e) Human Reliability Program (HRP) as required by Title 10 Code of Federal Regulations (CFR) Part 712, to ensure the reliability of DOE and contractor employees who require access to designated components, nuclear explosives, or nuclear weapons.
 - (f) Measures to prevent deliberate unauthorized acts, from degrading the effectiveness of UC measures incorporated in or used for nuclear explosives or nuclear weapons.
 - (g) Measures to prevent or delay DUU, deliberate unauthorized acts, DAU, or loss of control during planned NEOs.
 - (h) Measures to assist the recapture and recovery of lost or stolen nuclear explosives or nuclear weapons.
 - (i) Stockpile surveillance to ensure that UC devices and components meet specified requirements and have not been altered.
 - (j) Deliberate unauthorized act, DUU, and DAU evaluations performed periodically and documented that may be specific to a DOE nuclear weapon, nuclear explosive, NEO, class of operations, facility, or site (see also paragraph 2.c).

- (k) Measures that must be periodically assessed against existing and emerging threats as well as technological opportunities for improvement.
- (l) Security of the supply chain and protection against components and assemblies with malicious content that could override or degrade UC or nuclear weapons functionality.
- (m) Measures to ensure cyber security in all aspects of design, sourcing and coding, procurement, production, and sustainment to ensure that critical program information and systems are secure.
- (n) Necessary measures for interagency information sharing and cooperation in threat identification, supplier vetting, and risk mitigation.
- (o) Assessments that weapons systems, including associated systems and components/codes, have not been subverted or corrupted.
- (p) Records maintenance in accordance with National Archives and Records Administration-approved DOE or site-specific records retention schedules.
- (q) Research and Development (R&D) to protect against deliberate unauthorized acts, DUU, and DAU of nuclear explosives and nuclear weapons. Reference paragraph 2.e for required R&D program elements.
- (4) Ensure protection measures and program elements related to nuclear weapon design are consistent with DoD operational requirements.
- (5) Incorporate integrated risk management to ensure controls implemented to support the Nuclear Explosive Surety Standards for one aspect of surety (i.e., safety, security, UC, and digital assurance) are evaluated for adverse impact(s) on the other surety aspects.
- b. Nuclear Enterprise Assurance (NEA). NEA is an NSE countersubversion program established to detect and prevent subversion and mitigate the consequences of discovered subversions affecting nuclear weapons throughout their entire lifecycle, as well as to nuclear weapons enabling capabilities. NEA supports surety for Nuclear Explosives and Weapons, including providing assurance that components/systems are not subverted or compromised during design and production, in support of preventing deliberate unauthorized acts that may lead to DAU, or degradation of weapon reliability and/or performance. NEA increases system assurance for nuclear weapons and enabling capabilities, including digital assurance. DOE/NNSA must protect against adversarial subversion of the NSE supply chain; and evaluate documented evidentiary information that provides assurance that nuclear weapons and nuclear weapon-enabling capabilities have

not been subverted. Reference NNSA Supplemental Directive (NNSA SD) 452.4-1, *Nuclear Enterprise Assurance*, current version, for detailed NEA requirements.

- c. Deliberate unauthorized act, DUU, and DAU evaluations. Contractors must:
 - (1) Conduct evaluations for DOE/NNSA nuclear explosives, digital controls/codes, nuclear weapons, NEOs, and certain non-NEO production activities, assessing controls as they apply to the critical component, nuclear explosive, or nuclear weapons against credible existing and emerging threats and technological advancements to determine the adequacy of the controls. Reference NNSA SD 452.4, *Implementation and Evaluation of Controls to Prevent Deliberate Unauthorized Use*, current version, for additional direction for the evaluations.
 - (2) Evaluations must meet the following criteria:
 - (a) NNSA Sites with NEOs. The deliberate unauthorized act, DUU, and DAU evaluations will address NEO processes, testers, tooling, and facilities to ensure that controls are adequate to meet the UC elements of DOE O 452.1, current version, Nuclear Explosive Surety Standards applicable to NEOs.
 - (b) NNSA Sites without NEOs. The deliberate unauthorized act, DUU, and DAU evaluations will address DOE weapon component designs, testers, and subsystem/component production to ensure the integrity of product used in nuclear explosives and nuclear weapons is adequate so to not jeopardize conformance with the UC elements of DOE O 452.1, current version, Nuclear Explosive Surety Standards.
 - (3) Evaluations must be conducted in conjunction with the objectives of DOE O 470.3, *Design Basis Threat*, current version, to align with DOE's physical protection strategies.
 - (4) As requested by the Office of Stockpile Management (NA-12), contractors must provide technical support for DUU reviews and evaluations.
- d. Joint DOE/NNSA and DoD Collaboration. Contractors must:
 - (1) Collaborate with DoD as required to provide protection against deliberate unauthorized acts, DUU and DAU, and to assess the effectiveness of surety features for all U.S. nuclear weapon systems throughout their life cycles. These features must be consistent with DoD operational requirements and must continually be assessed against existing and emerging threats as well as technological opportunities for improvement.
 - (2) Assist DoD in designating nuclear command and control critical equipment and components to ensure that these items are developed and

maintained to meet the criteria designated in National Security Directives and the Nuclear Explosive and Weapon Surety (NEWS) and UC programs.

- e. Research and Development (R&D).
 - (1) Conduct R&D for security, digital assurance, and UC measures that can protect against deliberate unauthorized acts, DUU, and DAU of nuclear explosives and nuclear weapons, consistent with Nuclear Explosive Surety Standards and NEWS Program objectives prescribed in DOE O 452.1, current version.
 - (2) R&D for security, UC, and NEA must:
 - (a) Pursue technologies that can enhance security and UC for new and existing systems.
 - (b) Develop nuclear weapon measures to provide assurance of operation as designed when authorized for use.
 - (c) Design nuclear weapon features that enhance secure critical command and control communications.
 - (d) Develop technologies to aid in the recapture and recovery of weapons.
 - (e) Develop approaches to efficiently detect subversion.
 - (f) Ensure personnel responsible for R&D of security, UC, and NEA features appropriately protect as classified and controlled unclassified information (according to sensitivities) the improvements and information related to newly developed security, UC, and NEA measures.

ATTACHMENT 2 DEFINITIONS

Selected definitions from DOE O 452.1, current version, are repeated here for ease of reference.

1. Cybersecurity. The physical, technical, and administrative controls and risk management processes for providing the required and appropriate level of confidentiality, integrity, availability and accountability for DOE/NNSA information stored, processed, or transmitted on electronic systems (and networks).
2. Delay. The effect achieved by administrative controls, physical features, technical devices, security measures, or protective forces that impedes an adversary from gaining access to an asset being protected or from completing a malevolent act.
3. Deliberate Unauthorized Use (DUU). Any of the following consequences resulting from deliberate malevolent acts:
 - a. A nuclear explosive detonation that is not authorized by the National Command Authorities.
 - b. An HEVR that could result in an unauthorized nuclear explosive detonation.
 - c. Theft of nuclear explosives.
4. Denial of Authorized Use (DAU). Any unauthorized act, including deliberate unauthorized acts, that would prevent the authorized use or intended functionality of a nuclear weapon. The resulting potential effects on the nuclear weapon include but are not limited to:
 - a. Actual alteration of system or critical component functionality.
 - b. Perception that system or critical components are not functioning properly.
5. Digital Assurance. A term for practices, measures and/or controls applied to digital technologies that implement functions within a nuclear weapon (NW), or NW design, production, or test capability, in order to ensure functional, performance and security-related requirements are met while protecting against potential compromise or subversion of these same systems from internal or external sources. Examples of digital technologies include software/firmware, processors, memory devices, application-specific integrated circuits (ASICs), field programmable gate arrays (FPGAs), digital systems on a chip, communication interfaces, communication buses and transmission systems, etc.
6. Measures. The total spectrum of characteristics, devices, equipment, procedures, and administrative processes used to ensure timely authorized use only when directed by national authority, and to increase the difficulty of or add to the delay in achieving the deliberate unauthorized use of a nuclear explosive.

7. Nuclear Command and Control Critical Equipment. Specifically designated equipment, including software, used to build, encode, decode, transmit, or receive emergency action messages; identify nuclear targets, select nuclear weapons to be used against specific targets, and route nuclear-weapons-carrying platforms to appropriate launch points; and support or inhibit the delivery, arming, fusing, and firing of nuclear weapons themselves. This equipment includes positive control material and devices, and nuclear weapon hardware.
8. Nuclear Enterprise Assurance (NEA). A Nuclear Security Enterprise (NSE) countersubversion program established to prevent, detect and/or mitigate potential consequences of subversion of nuclear weapons (NWs) or the enabling capabilities throughout the NW lifecycle, including deliberate unauthorized acts that may lead to denial of authorized use (DAU) or degradation of nuclear weapon reliability or performance.
9. Nuclear Enterprise Assurance Steering Group (NEASG). A review and decision-making body consisting of senior federal officials from NNSA and DOE Headquarters who provide leadership regarding NEA activities, including facilitating collaboration with the Department of Defense (DoD).
10. Nuclear Explosive. An assembly containing fissionable and/or fusionable materials and main charge high-explosive parts or propellants capable of producing a nuclear explosive detonation (e.g., a nuclear weapon or test device).
11. Nuclear Explosive Operation (NEO). Any activity involving a nuclear explosive including activities in which main charge high-explosive parts and pit are collocated.
12. Nuclear Security Enterprise (NSE). The collection of DOE laboratories, Nevada National Security Site, production plants, and processing facilities involved in the design, production, and testing of nuclear weapons.
13. Nuclear Weapon (NW). A nuclear explosive configured for Department of Defense use.
14. Nuclear Weapon Crosscutting Functions and Programs. Functions and programs implemented across the NSE to enable and support nuclear weapon capabilities, that use controls and measures to detect, prevent, or minimize the effects of subversion in support of NEA, such as supply chain risk management (SCRM), cybersecurity, information security, verification and acceptance, information management, logistics, physical security, and quality assurance.
15. Nuclear Weapon (NW) Enabling Capabilities. The infrastructure (facilities, utilities, and workforce), processes, equipment, materials, and tools that provide the NSE the ability to ensure reliability and performance of the NW stockpile throughout its lifecycle, including those needed to support procurement, management, research and development (R&D), design, production, testing, surveillance, maintenance, transport, dismantlement, and disposition of NWs or NW components.

16. Recapture. Regaining control of a nuclear weapon or special nuclear material, which is under unauthorized possession, while still within the confines of a Departmental site/facility.
17. Recovery. Regaining control of a nuclear weapon or special nuclear material, which is under unauthorized possession and has been removed from within the confines of a Departmental site/facility or Departmental possession.
18. Security. An integrated system of activities, systems, programs, facilities, and policies for the protection of classified information or classified matter, controlled unclassified information, nuclear materials, nuclear weapons, nuclear weapon components, or the DOE's and its contractors' facilities, property, and equipment.
19. Surety. Safety, security, and use control of nuclear explosives and nuclear weapons.
20. System Assurance. The justified confidence that the system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during the lifecycle. (Source: NATO. 2010. Engineering for system assurance in NATO programs. DoD 5220.22M-NISPOM-NATO-AEP-67. February 2010.)
21. Unauthorized Act. Any action that has not been authorized and approved by proper authority. In the context of the Nuclear Explosive Surety Standards, an Unauthorized Act is one that is not sanctioned as part of an approved NEO or associated activity, but which could affect a nuclear explosive or main charge high explosive part in a Nuclear Explosive Area. Unauthorized Acts may be characterized as deliberate or unintended, and as either malevolent or non-malevolent.
 - a. From a NES perspective, an Unauthorized Act is of interest if performed without intent to compromise nuclear explosive surety (i.e., non-malevolent). This includes cognitive errors (errors of omission or commission) and accidental or inadvertent acts.
 - b. From a use control perspective, an Unauthorized Act is of interest if it is both deliberate and malevolent. More specifically, an act performed with intent to create an unauthorized nuclear explosive detonation or to gain unauthorized control of a nuclear explosive.
22. Use Control (UC). The application of systems, devices, or procedures that ensure timely authorized use of a nuclear explosive while precluding or delaying unauthorized nuclear detonation.

ATTACHMENT 3 REFERENCES

1. 10 CFR Part 712, *Human Reliability Program*, the rule that defines a security and safety reliability program designed to ensure that individuals who occupy positions affording access to certain materials, nuclear explosive devices, facilities, and programs meet the highest standards of reliability and physical and mental suitability.
2. 10 CFR Part 1017, *Identification and Protection of Unclassified Controlled Nuclear Information*.
3. 10 CFR 1045, *Nuclear Classification and Declassification*.
4. Presidential Policy Directive (PPD)-35, *United States Nuclear Command Control, Safety and Security*, dated 12-8-15.
5. *Joint Policy Statement on Nuclear Weapons Surety*, dated 6-27-91, signed by the Secretary of Defense and the Secretary of Energy.
6. *Memorandum of Understanding Between the Department of Defense and Department of Energy on Objectives and Responsibilities for Joint Nuclear Weapon Activities*, dated 1-17-83, which supplements previous agreements delineating DoD and DOE objectives, responsibilities, and measures to improve stockpile planning and acquisition and ensuring high-level attention to nuclear weapon safety, security, and UC.
7. CJCSI 3260.01D, *Joint Policy Governing Positive Control Material and Devices*, is a directive that establishes National policy and procedures applicable to the Executive Branch for positive control material and devices. It is the source document and authorization for TP 50-2. Classified.
8. Technical Manual (TP) 50-2, *Procedures for the Use and Control of Logistics Codes for Permissive Action Link (PAL) Equipped Weapons*, is a joint DOE and DoD directive that provides the policies, requirements and technical procedures for handling and controlling of logistics code and key material. Classified.
9. DOE P 470.1, *Safeguards and Security Program*, current version, ensures that DOE efficiently and effectively meets all its obligations to protect Special Nuclear Material, other nuclear materials, classified matter, sensitive information, government property, and the safety and security of employees, contractors, and the general public.
10. DOE O 151.1, *Comprehensive Emergency Management System*, current version, provides the framework for development, coordination, control, and direction of all emergency planning, preparedness, readiness assurance, response, and recovery actions.
11. DOE O 205.1, *Department of Energy Cybersecurity Program*, current version, enables accomplishment of the Department's mission and fulfill Federal cybersecurity

requirements while allowing Departmental Elements (DEs) programmatic and operational flexibility.

12. DOE O 226.1, *Implementation of Department of Energy Oversight Policy*, current version, implements the policy that establishes a Department-wide oversight process to protect the public, workers, environment, and national security assets effectively through continuous improvement.
13. DOE O 243.1, *Records Management Program*, current version, provides a framework for managing information and National Archives and Records Administration approved DOE or site-specific records schedules.
14. DOE O 251.1, *Departmental Directives Program*, current version, establishes directives as the primary means to set, communicate, and institutionalize policies, requirements, responsibilities, and procedures for Departmental elements and contractor.
15. DOE O 414.1, *Quality Assurance*, current version, ensures that DOE, including NNSA, products, and services meet or exceed customers' requirements and expectations.
16. DOE O 452.1, *Nuclear Explosive and Weapon Surety Program*, current version, establishes the Nuclear Explosive and Weapon Surety (NEWS) Program to prevent unintended/unauthorized detonation and deliberate unauthorized use of nuclear explosives, as well as specifying Nuclear Explosive Surety Standards.
17. DOE O 452.2, *Nuclear Explosive Safety*, current version, establishes requirements to implement the nuclear explosive safety (NES) elements of DOE O 452.1, *Nuclear Explosive and Weapon Surety (NEWS) Program*, current version, for routine and planned nuclear explosive operations (NEOs) and nuclear explosive-like assemblies (NELAs).
18. DOE O 452.6, *Nuclear Weapon Surety Interface with the Department of Defense*, current version, establishes Department of Energy and National Nuclear Security Administration requirements and responsibilities for addressing joint nuclear weapon and nuclear weapon system surety activities in conjunction with the Department of Defense.
19. DOE O 461.1, *Packaging and Transportation for Offsite Shipment of Materials of National Security Interest*, current version, makes clear that the packaging and transportation of all offsite shipments of Materials of National Security Interest (MNSI) for DOE must be conducted in accordance with Department of Transportation (DOT) and Nuclear Regulatory Commission (NRC) regulations that would be applicable to comparable commercial shipments, except where an alternative course of action is identified.
20. DOE O 470.3, *Design Basis Threat*, current version. Classified.
21. DOE O 470.4, *Safeguards and Security Program*, current version, establishes roles and responsibilities for the Department of Energy Safeguards and Security Program.

22. DOE O 471.1, *Identification and Protections of Unclassified Controlled Nuclear Information*, current version, provides requirements and responsibilities for identifying and protecting the unauthorized dissemination of Unclassified Controlled Nuclear Information.
23. DOE O 471.6, *Information Security*, current version, establishes requirements and responsibilities for DOE Departmental Elements, including the NNSA, to protect and control classified information as required by statutes, regulation, Executive Orders, government-wide policy directives and guidelines, and DOE policy and directives.
24. DOE O 475.2, *Identifying Classified Information*, current version, establishes the program to identify information classified under the Atomic Energy Act or Executive Order (E.O.) 13526 so that it can be protected against unauthorized dissemination.
25. NNSA SD 452.4, *Implementation and Evaluation of Controls to Prevent Deliberate Unauthorized Use*, current version, supports this Order's requirements to implement deliberate unauthorized use (DUU) preventive measures for nuclear explosive operations (NEO) and associated activities and to perform independent evaluations to determine if NEOs are adequately designed and controlled to satisfy the use control (UC) Standard of DOE O 452.1, *Nuclear Explosive and Weapon Surety (NEWS) Program*, current version, and the DUU control criteria.
26. NNSA SD 452.4-1, *Nuclear Enterprise Assurance*, current version, establishes NEA as a NSE countersubversion program to prevent, detect, and/or mitigate potential consequences of subversion of nuclear weapons (NWs) and NW-enabling capabilities to prevent deliberate unauthorized acts that may lead to Denial of Authorized Use (DAU) or degradation of nuclear weapon reliability or performance, in support of implementing DOE O 452.1, *Nuclear Explosive and Weapon Surety (NEWS) Program*, and DOE O 452.4, *Security and Use Control of Nuclear Explosives and Nuclear Weapons*, requirements.
27. *DOE/DOD Procedures for Assessment of Use Control Effectiveness*, dated 1-28-81.