SUPPLEMENTAL DIRECTIVE

NNSA SD 452.4-1

Approved: 01-27-22
Expires: 01-27-25

NUCLEAR ENTERPRISE ASSURANCE (NEA)

NATIONAL NUCLEAR SECURITY ADMINISTRATION
Office of Defense Programs

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

OFFICE OF PRIMARY INTEREST (OPI):
Office of Stockpile Production Integration

printed copies are uncontrolled

THIS PAGE INTENTIONALLY LEFT BLANK

NUCLEAR ENTERPRISE ASSURANCE (NEA)

1. PURPOSE. To support implementation of Department of Energy (DOE) Order (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*. Consistent with the parent directive requirements, Nuclear Enterprise Assurance (NEA) is a Nuclear Security Enterprise (NSE) countersubversion program established to prevent, detect, and/or mitigate potential consequences of subversion of nuclear weapons (NWs) and NW-enabling capabilities, including Deliberate Unauthorized Acts (DUAs), that may lead to Denial of Authorized Use (DAU) or degradation of NW reliability or performance. Credible existing and emerging threats and technological advancements are evaluated, and controls and measures are implemented by federal and contractor NSE organizations, to manage NEA-related risks and provide assurance that NWs, NW-enabling capabilities, and NW crosscutting functions and programs, have not been subverted throughout the NW lifecycle.

   The primary objectives of this SD include:

   a. Establishing concise NEA requirements to ensure consistent and coordinated NSE-wide federal and Management and Operating (M&O) contractor application of NEA to:

      (1) NW programs throughout the NW lifecycle (new development, sustainment, modernization, and retirement);

      (2) NW-enabling capabilities, which include 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; and

      (3) NW crosscutting functions and programs implemented across the NSE to support NW programs and enabling capabilities, such as supply chain risk management (SCRM), cybersecurity, information security, verification and acceptance, information management, logistics, physical security, and quality assurance.

   b. Expanding upon the roles and responsibilities of the Nuclear Enterprise Assurance Steering Group (NEASG) that was instituted by DOE O 452.4 to provide leadership for NEA activities; and

   c. Establishing the NEA Integration Working Group (NIWG) as the principal M&O entity for developing, integrating, and coordinating NEA initiatives and activities across the NSE, including specifying the NIWG roles, responsibilities, and functions.

2. AUTHORITY. This SD augments and aligns with DOE O 452.4, *Security and Use Control of Nuclear Explosives and Nuclear Weapons*, and DOE O 452.1, *Nuclear Explosive and Weapon Surety (NEWS) Program.*

3. CANCELLATIONS.

a. NNSA Policy (NAP-401.1), *Weapon Quality Policy*, Attachment 4, *Nuclear Enterprise Assurance (NEA)*, dated November 24, 2015.

b. Memorandum, Donald Cook to NSE, *Nuclear Enterprise Assurance Program Guidance*, 08-4-14.

c. Memorandum, William S. Goodrum to NSE, *Nuclear Enterprise Assurance Guidance*, 10-21-14.

Cancellation of a directive does not, by itself, modify or otherwise affect any contractual obligation to comply with the directive listed above. Contractor Requirements Documents (CRDs) that have been incorporated into a contract remain in effect throughout the term of the contract until the contract or regulatory commitment is modified to either eliminate outdated requirements or substitute new requirements.

4. APPLICABILITY.

a. Federal. This SD applies to all NNSA Federal organizations responsible for maintaining and enhancing the safety, reliability, and performance of the United States (U.S.) NW stockpile, including the ability to design, produce, and test NWs in order to meet national security requirements.

b. Contractors. The Contractor Requirements Document (CRD), provided as Attachment 1, sets forth requirements that apply to the M&O contractors. The CRD must be included in the contracts of NSE M&O contractors that support the NNSA mission to maintain and enhance the safety, reliability, and performance of the U.S. NW stockpile, including the ability to design, produce, and test NWs in order to meet national security requirements.

c. Equivalencies/Exemptions.

(1) Equivalency. In accordance with the responsibilities and authorities assigned by Executive Order 12344, codified at 50 United States Code, 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.

(2) Exemption. None.

5. SUMMARY OF CHANGES. Not applicable

6. BACKGROUND.

The world threat environment is continuously changing, requiring the NSE national laboratories and production facilities to respond accordingly. Government agencies have mobilized under a variety of national-level directives to protect critical security elements against a broad spectrum of adversarial threats. The U.S. Government is concerned about the globalization of today's NW supply chains, especially when coupled with increasingly sophisticated adversaries. Additional areas of concern include global development and sourcing of microelectronics and software, as well as the supply chains of other NW-related materials or products that could be maliciously altered. The increasing complexity of NW information technology presents challenges for organizations to assure the safety, reliability, and security of those technologies, due to their vulnerability to subversion, corruption, denial of service, and other cyberattacks. It is recognized that defensive measures must reflect an appreciation for the rapidly evolving, persistent, and aggressive approaches an adversary may employ in order to affect the NSE mission.

NEA is the NSE program established to prevent, detect, and/or mitigate potential consequences of subversion, including DUA that may lead to DAU or degradation of weapon reliability or performance. NEA is intended to reduce the risk of subversion by advanced persistent threats and other adversaries that possess the expertise and resources that enable them to create and exploit subversion opportunities. NEA includes the systematic identification, assessment, and mitigation of subversion risks, based on analysis of vulnerabilities and adversarial threats, to provide assurance that NWs, NW-enabling capabilities, and NW crosscutting functions and programs are not subverted or compromised throughout the NW lifecycle.

7. REQUIREMENTS.

When reviewing the following federal requirements, it is important to acknowledge, that in the context of DOE/NNSA Directives/Policies, "*prevent*" and "*ensure*" imply an absolute assurance, which cannot be guaranteed. The objective is to evaluate credible existing and emerging threats and technological advancements and implement controls and measures to prevent, detect, and mitigate the consequences of subversion. This enables management of NEA-related risks and provides reasonable assurance that the NW stockpile, enabling capabilities, and crosscutting functions and programs, including NSE supply chains, have not been subverted and that the NW stockpile is protected against DUA that may lead to DAU or loss of NW reliability or performance.

a. NNSA must ensure NWs, NW-enabling capabilities and NW crosscutting functions and programs are secured from subversion throughout the NW lifecycle.

b. NNSA must establish and implement oversight and monitoring/measuring of NEA assurance.

c. Enterprise-wide policies and procedures must be developed and executed to ensure NEA implementation by federal organizations and M&O contractors

throughout the NW lifecycle, including NW-enabling capabilities and crosscutting functions and programs, to include the following:

(1) Common documented methodologies for implementing digital assurance processes;

(2) Common documented methodologies for implementing NW system assurance processes; and

(3) An NEA risk management methodology that:

(a) Assesses threats, vulnerabilities, and consequences from credible existing and emerging adversarial subversion;

(b) Identifies potential controls and measures to prevent, detect, and mitigate the consequences of subversion; and

(c) Is integrated with NNSA Defense Programs (DP) risk management processes and protocols to inform decisions regarding NEA-related risks.

d. NNSA must evaluate, prioritize, and oversee the implementation of NEA controls and measures identified throughout the NW lifecycle by the M&O contractors for NWs, NW-enabling capabilities, and NW crosscutting functions and programs.

e. Processes, controls, and measures must be established and implemented to protect against adversarial subversion within NSE supply chains.

f. NW design must be innovated to enhance resiliency against threats and vulnerabilities to provide increased system assurance.

g. NEA R&D activities must be conducted to develop and mature new methods, techniques, tools, and expertise to prevent, detect, and mitigate the effects of subversion.

h. NEA-related risks must be evaluated, and controls and measures implemented, when designing, building, operating, or modifying NSE facilities for NW-enabling capabilities.

i. An NEA Steering Group (NEASG) must be formed and implemented, consistent with DOE O 452.4, to perform the following functions:

(1) Make NEA-related decisions and recommendations to sustain NEA implementation and drive uniformity and consistency within DP;

(2) Work with other governmental entities, including the Department of Defense (DOD), to promote collaboration across acquisition; research, development, test, and evaluation (RDT&E); production,

operation; and sustainment efforts to facilitate effective planning, coordination and execution of NEA capabilities, protections, and investments across the NSE throughout the NW lifecycle;

(3) Promote coordination and sharing of information between DOE, NNSA, DOD, and the necessary subject matter experts in order to enhance threat identification, supplier evaluation, and risk management of NEA-related issues; and

(4) Integrate and coordinate NEA activities across the NSE and address critical, high-priority NEA topics and areas, through the NIWG.

j. An integrated approach to NEA activities must be established, including the capability to respond to enterprise-wide and site-level NEA issues.

k. NNSA must obtain intelligence and counterintelligence support for NEA activities from the DOE Office of Intelligence and Counterintelligence (DOE-IN), consistent with DOE O 452.4, to fulfill the requirements of this SD.

l. Evidentiary information must be required to demonstrate that NEA implementation is continually evaluated, managed, and documented throughout the NW lifecycle.

m. NNSA must collaborate with the NIWG.

n. NNSA must develop NEA training standards and ensure that corresponding NEA training is developed and delivered to the NSE workforce to enable effective execution of NEA requirements.

8. RESPONSIBILITIES.

a. Assistant Deputy Administrator for Stockpile Management (ADASM/NA-12)

In addition to the NEA responsibilities in DOE O 452.1 and DOE O 452.4, the ADASM is responsible for:

(1) Ensuring that DP NEA processes are developed, maintained, and managed to implement the requirements of this SD; and

(2) Accepting NEA-related risks on behalf of the Deputy Administrator for Defense Programs throughout the NW lifecycle, e.g., sustainment of stockpile systems and stockpile modernization (life extension programs (LEPs), Alterations (Alts), and Modifications (Mods), unless otherwise delegated.

b. Office of Research, Development, Test, and Evaluation (RDT&E/NA-11)

In addition to the NEA responsibilities in DOE O 452.1 and DOE O 452.4, the Office of RDT&E is responsible for:

(1) Promoting development of innovative technologies for detecting, testing, analyzing, and protecting against vulnerabilities associated with adversarial subversion; and

(2) Supporting expanded development of NEA resources, including technology maturation, vulnerability analysis tools, and evidence-based practices.

c. Office of Stockpile Production Integration (NA-121)

In addition to the NEA responsibilities in DOE O 452.4, the Office of Stockpile Production Integration is responsible for:

(1) Establishing, maintaining, and supporting the DOE/NNSA Directives that govern NEA implementation;

(2) Developing, maintaining, and managing DP NEA processes to implement the requirements of this SD;

(3) Monitoring and evaluating NNSA and M&O contractor performance of NEA requirements, in collaboration with the NNSA Field/Production Offices (F/POs);

(4) Providing communications and information to the NEASG, as requested, and serving as the secretariat for the NEASG;

(5) Establishing and implementing a response capability for enterprise-wide and site-level NEA issues;

(6) Developing NEA standards and processes for NSE-wide NEA awareness, training, and skills development;

(7) Collaborating with the NIWG, including providing communications, information, and other support;

(8) Serving as the NEA federal integrator in collaboration with the NSE sites, the DOD, and other stakeholders; and

(9) Coordinating with DOE-IN, as needed, to support NEA Program needs.

d. Federal Program Managers (FPMs)

This SD applies to FPMs responsible for managing NW programs; NW-enabling capabilities; and NW crosscutting functions and programs, throughout the NW lifecycle.

(1) *FPMs for the NW-enabling capabilities and NW crosscutting functions and programs* are responsible for:

(a) Evaluating NEA threats and vulnerabilities for their respective programs/projects/facilities against credible existing and emerging adversarial subversion.

(b) Identifying NEA-related risks and implementing controls and measures to prevent, detect, and mitigate the effects of subversion.

(2) *FPMs for NW programs* (e.g., active stockpile, LEPs, Alts, Mods, new development, etc.) are responsible for:

(a) Integrating innovated NEA concepts/components into the NW design (new and modified NWs).

(b) Leveraging the NEA controls and measures being applied in the NW-enabling capabilities and crosscutting functions and programs, and evaluating their respective project/program in order to:

1 Evaluate NW threats and vulnerabilities to identify risks from credible existing and emerging adversarial subversion;

2 Determine if the controls and measures being applied in the NW-enabling capabilities and crosscutting functions and programs provide adequate assurance that their respective NW program is secure from subversion; and

3 Implement additional NEA controls and measures, as appropriate.

(c) Integrating and managing NEA subversion risks and associated controls and measures within their respective project/program risk management process(es).

(3) Additionally, *all FPMs* are responsible for:

(a) Including NEA requirements in program budgets and contracts;

(b) Managing NEA-related risks for their respective program, capability or function throughout the NW lifecycle, including

implementing NEA controls and measures to protect the NWs, NW-enabling capabilities and NW crosscutting functions and programs from subversion;

(c) Collaborating/partnering with other FPMs when there are common or overlapping NEA-related risks;

(d) Supporting implementation of innovative technologies for detecting, testing, analyzing, and protecting against vulnerabilities associated with adversarial subversion; where feasible; and

(e) Accepting project/program NEA-related risks, if delegated from the ADASM.

e. Field/Production Office (F/PO) Contracting Officers (COs)

Incorporate this SD into the "List of Applicable Directives" identified in the "Laws, Regulations, and DOE Directives" clause of the M&O contracts for NSE M&O Contractors that perform work in support of the NNSA mission to maintain and enhance the safety, reliability, and performance of the U.S. NW stockpile, including the ability to design, produce, and test NWs in order to meet national security requirements.

f. NEA Steering Group (NEASG)

The NEASG is a review and decision-making body, instituted by DOE O 452.4, consisting of senior DOE and NNSA officials who provide leadership and promote successful execution of NEA. As established by DOE O 452.4, the NEASG is overseen by the ADASM and consists of senior members from DOE-IN, the NNSA Office of Defense Nuclear Security (NA-70), the NNSA Office of Information Management and Chief Information Officer (NA-IM), as well as the NNSA Defense Programs Associate Deputy Administrators. Other NEASG members can be added at the discretion of the ADASM.

The NEASG is responsible for:

(1) Decision-making for NEA-related initiatives or issues requiring uniformity or consistency across the NSE;

(2) Facilitating collaboration across acquisition, RDT&E, operation, and sustainment efforts to enable effective planning, coordination, and execution of NEA capabilities and investments across the DOE/NNSA, DOD and, to the extent possible, with other U.S. Government partners;

(3) Promoting coordination and sharing of information between DOE, NNSA, DOD, and the necessary subject matter experts in order to

enhance threat identification, supplier evaluation, and risk management of NEA-related issues; and

(4) Resolving conflicts between NNSA organizations at the appropriate management level.

9. DEFINITIONS. See Attachment 2.

10. ACRONYMS/ABBREVIATIONS. See Attachment 3.

11. REFERENCES.

a. 50 U.S. Code 2401, Section 3202, *The National Nuclear Security Administration Act.*

b. DOE O 452.1E, *Nuclear Explosive and Weapon Surety Program*, dated 01-26-15

c. DOE O 452.4C, *Security and Use Control of Nuclear Explosives and Nuclear Weapons*, dated 08-28-15.

d. NAP 401.1, *Weapon Quality Policy*, Attachment 4, (*Nuclear Enterprise Assurance*), dated 11-24-15.

e. NAP 476.1, *Atomic Energy Act Control of Import and Export Activities*, dated 02-09-15.

f. NNSA Redelegation Order No. NA-005.01-01, dated 03-25-19

12. CONTACT.

DOE/NNSA Nuclear Enterprise Assurance Division, NA-121.4, (505) 845-5750

BY ORDER OF THE ADMINISTRATOR:

Jill Hruby
Administrator

Attachments:

1. Contractor Requirements Document (CRD)
2. Definitions
3. Acronyms/Abbreviations

THIS PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT 1: CONTRACTOR REQUIREMENTS DOCUMENT

This Management and Operating (M&O) Contractor Requirements Document (CRD) establishes Nuclear Enterprise Assurance (NEA) requirements for M&O contractors within Nuclear Security Enterprise (NSE) sites or facilities that support the National Nuclear Security Administration (NNSA) mission to maintain and enhance the safety, reliability, and performance of the U.S. Nuclear Weapon (NW) stockpile, including the ability to design, produce, and test NWs in order to meet national security requirements. The NSE M&O contractors with Supplemental Directive (SD) 452.4-1 on their contract are responsible for complying with the requirements of this CRD and for flowing down the requirements of this CRD to subcontractors, at any tier, to the extent necessary to ensure compliance with the requirements.

When reviewing the following requirements, it is important to acknowledge that in the context of DOE/NNSA Directives/Policies, "prevent" and "ensure" imply an absolute assurance, which cannot be guaranteed. The objective is to evaluate credible existing and emerging threats and technological advancements and implement controls and measures to prevent, detect, and mitigate the consequences of subversion in order to manage NEA-related risks and provide reasonable assurance that the NW stockpile, NW-enabling capabilities, and NW crosscutting functions and programs, are protected against Deliberate Unauthorized Acts (DUA) that may lead to Denial of Authorized Use (DAU) or loss of weapon reliability and/or performance.

1. REQUIREMENTS.

   a. M&O contractors must develop and implement common documented NSE methodologies that address the applicable elements needed to protect NWs, NW-enabling capabilities, and NW crosscutting functions and programs, to include:

      (1) NEA digital assurance processes;

      (2) NW system assurance processes; and

      (3) Management of NEA-related risks, including:

         (a) Evaluating risks from credible existing and emerging threats and technological advancements;

         (b) Identifying potential controls and measures to prevent, detect, and mitigate the consequences of subversion; and

         (c) Integrating NEA-related risks with NSE risk management processes to inform NNSA NEA risk handling decisions.

   b. M&O contractors must establish self-governance processes and implement line management accountability for ensuring the implementation of this CRD at their respective sites, including their respective subcontractors.

c. M&O contractors must innovate NW design to increase resiliency against adversarial subversion threats and provide increased system assurance.

d. M&O contractors must establish and implement processes, controls, and measures to protect against adversarial subversion within the NSE supply chains.

e. M&O contractors must develop and mature new technologies and capabilities for preventing, detecting, and minimizing the impacts of adversarial subversion.

f. M&O contractors must evaluate NEA risk and implement controls and measures when designing, building, operating, or modifying NW-enabling capabilities.

g. M&O contractors must support NEA Integration Working Group (NIWG) activities, including:

(1) Appointing senior-level knowledgeable personnel with decision-making authority to participate in the NIWG;

(2) Providing NEA recommendations and guidance to NNSA;

(3) Addressing critical, high-priority NEA topics/areas;

(4) Integrating and coordinating NEA activities, controls, and measures across the NSE;

(5) Facilitating communication of NEA information, including best practices; and

(6) Performing routine reviews of NEA implementation activities at the NSE sites to identify best practices and areas for improvement.

h. M&O contractors must develop NEA-related training that implements the NNSA-developed NEA training standards, and train appropriate personnel, consistent with their respective NEA responsibilities.

i. M&O contractors must establish and document a process for NEA records management that complies with DOE Order (O) 243.1, *Records Management Program*.

j. M&O contractors must coordinate, develop, and implement strategies for collaborating with NNSA, DOE Office of Intelligence and Counterintelligence (DOE-IN), and the intelligence community (e.g., counterintelligence and the field intelligence element) to conduct NEA analyses related to NWs and NW-enabling capability requirements at their respective sites, consistent with DOE O 452.4C.

k. M&O contractors must establish and implement processes for NSE-wide collaboration and information sharing to facilitate threat identification, supplier vetting, and risk management of NEA-related issues.

l. M&O contractors must conduct NEA vulnerability assessments that consider credible existing and emerging threats and technological advancements to manage NEA protections/controls for NWs, NW-enabling capabilities, and NW crosscutting functions and programs.

m. M&O contractors must document NEA controls and measures for NWs that leverage the vulnerability assessments of the NW-enabling capabilities and NW crosscutting functions and programs.

n. M&O contractors must provide evidentiary information to demonstrate that NEA implementation is continually evaluated, measured, managed, and documented throughout the NW lifecycle.

o. M&O contractors must provide NEA support and personnel resources to the NSE Product Realization Process to ensure implementation of NEA during the NW lifecycle, including the NW-enabling capabilities and NW crosscutting functions and programs.

p. M&O contractors must implement a process to manage potential NEA-related anomalies and non-conformances with the consideration that the non-conformance may have been the result of an intentional adversarial action, ensuring appropriate classification requirements and controls are used while evaluating and analyzing nonconforming conditions.

q. M&O contractors must support the NNSA-directed response capability to respond to enterprise and site-wide NEA issues, consistent with NNSA funding and resources.

ATTACHMENT 2: DEFINITIONS

Note: This attachment applies to NNSA federal and M&O contractor personnel.

1. Digital Assurance. 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, field programmable gate arrays, digital systems on a chip, communication interfaces, communication buses, and transmission systems, etc.

2. Measures. The total spectrum of characteristics, devices, equipment, procedures, and administrative processes used to:

   a. Ensure timely authorized use only when directed by national authority, and

   b. Increase the difficulty of, or add to the delay in, achieving the deliberate unauthorized use of a nuclear explosive.

3. Nuclear Enterprise Assurance (NEA). A Nuclear Security Enterprise (NSE) countersubversion program established to prevent, detect, and/or mitigate potential consequences of subversion of NWs or the enabling capabilities throughout the NW lifecycle, including Deliberate Unauthorized Acts (DUA) that may lead to Denial of Authorized Use (DAU) and/or degradation of weapon reliability or performance.

4. Nuclear Enterprise Assurance (NEA) Integration Working Group (NIWG). A collection of Management and Operating (M&O) contractor experts and leadership representing each of the NSE sites, that is responsible for providing NEA recommendations and guidance to NNSA, responding to NEA issues and challenges across the Nuclear Security Enterprise, integrating NEA activities, facilitating communication of NEA best practices and information, and collaborating with a variety of organizations and groups (e.g., intelligence, counterintelligence, security, technical communities, and NNSA customers) in support of protecting the nation's NW stockpile from subversion by adversarial threats.

5. 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).

6. Nuclear Weapon (NW) crosscutting functions and programs. Functions and programs implemented across the NSE to enable and support NW capabilities, that use controls and measures to detect, prevent, and/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.

7. 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.

8. 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)

ATTACHMENT 3: ACRONYMS/ABBREVIATIONS

a.	ADASM	Assistant Deputy Administrator for Stockpile Management
b.	AEP	Allied Engineering Procedure
c.	Alt	Alteration
d.	CRD	Contractor Requirements Document
e.	DAU	Denial of Authorized Use
f.	DOE	Department of Energy
g.	DP	Defense Programs
h.	DUA	Deliberate Unauthorized Act
i.	F/PO	Field/Production Office
j.	FPM	Federal Program Manager
k.	LEP	Life Extension Program
l.	M&O	Management and Operating
m.	Mod	Modification
n.	NA	NNSA Office Designation
o.	NAP	NNSA Policy
p.	NATO	North Atlantic Treaty Organization
q.	NEA	Nuclear Enterprise Assurance
r.	NEASG	Nuclear Enterprise Assurance Steering Group
s.	NISPOM	National Industrial Security Program Operating Manual
t.	NIWG	NEA Integration Working Group
u.	NNSA	National Nuclear Security Administration
v.	NSE	Nuclear Security Enterprise

w.	NW	Nuclear Weapon
x.	R&D	Research and Development
y.	RDT&E	Research, Development, Test, and Evaluation
z.	SCRM	Supply Chain Risk Management
aa.	SD	Supplemental Directive