

SUPPLEMENTAL DIRECTIVE

NNSA SD 470.4-2

Approved: 06-23-18
Admin. Change 1: 06-16-21
Certification Due: 06-16-24

ENTERPRISE SAFEGUARDS AND SECURITY PLANNING AND ANALYSIS PROGRAM



**NATIONAL NUCLEAR SECURITY ADMINISTRATION
Office of Defense Nuclear Security**

**CONTROLLED DOCUMENT
AVAILABLE ONLINE AT:
<https://directives.nnsa.doe.gov>**

**OFFICE OF PRIMARY INTEREST:
Office of Defense Nuclear Security**

printed copies are uncontrolled

**June 16, 2021 Administrative Change 1 to
NNSA SD 470.4-2, *Enterprise Safeguards and Security Planning and Analysis***

Page	Paragraph	Changed
Page 8	5. v.	Deleted “The E-SSPAP Program Manager will generate an annual report documenting the status of security across the nuclear security enterprise.”
Page 10	6. c. (4)	Deleted, “...prior to approval by the ODFSA.”
Page 10	Footnote	Deleted after “...and SRAs.” “...and SPs. The SSP will be reviewed by NA-70 after the document is approved by the Field Office Manager.”
Page 11	c. (7) (e)	Deleted “Site security plans;”
Page 12	6. f. (3)	Added “SSPs and”
Page 12	6. f. (9)	Approves the PF Rules of Engagement – Deleted “after consultation with NA-71 and NNSA General Counsel.”
Page 20	1. y.	Deleted “The E-SSPAP Program Manager will generate an annual report documenting the status of security across the nuclear security enterprise.”
Page 21	6. f. (3)	Added “SSPs and”
Page 24	Attachment 2	Second paragraph, end of sentence – Deleted “, and site security plans.”
Page 25	Table Item 6	Removed NA-71 from Reviewing Org(s) column, and “Not Required” from Prior to Approval column.
Page 25	Footnote	Deleted footnote 4
Page 26	Table Item 6 (Scoping Agreements)	Changed N/A to NA-71 and add footnote 5. Program review process fulfills the review requirements for NA-71.

THIS PAGE INTENTIONALLY LEFT BLANK

ENTERPRISE SAFEGUARDS AND SECURITY PLANNING AND ANALYSIS PROGRAM

1. PURPOSE. This National Nuclear Security Administration (NNSA) Supplemental Directive (SD) prescribes the Defense Nuclear Security (DNS) Enterprise Safeguards and Security Planning and Analysis Program (E-SSPAP) process used to develop a standardized procedure for conducting a security risk assessment (SRA) or vulnerability assessment (VA) and reporting risk within the NNSA nuclear security enterprise.

This SD supplements Department of Energy (DOE) Order (O) 470.4, *Safeguards and Security Program* by providing a standardized approach to security risk management. This approach is required to provide a consistent set of deliverables to effect risk-informed decisions that result in an integrated, robust, effective, and efficient safeguards and security program. This SD provides the framework necessary to create those deliverables.

2. CANCELLATION. None.

3. APPLICABILITY.

- a. Federal. This SD and Attachment 2 applies to all NNSA elements.

- b. Contractors. The Contractor Requirements Document (CRD) provided as Attachments 1 and 2 sets forth the requirements of this directive that apply to contractors conducting safeguards and security activities. The CRD must be included in contracts of Management and Operating (M&O) and all prime contractors performing safeguards and security work for NNSA.

- c. Equivalencies.

- (1) Kansas City National Security Campus will implement the CRD in accordance with the approved federal oversight model established under the Administrator's letter dated April 12, 2006.

- (2) 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.

- d. Exemptions.

- (1) This SD does not apply to the Office of Secure Transportation.

- (2) All other deviations or exemptions to this SD must be sent through federal channels to Defense Nuclear Security (NA-70).

4. BACKGROUND. DNS had the need for a standard and consistent security risk management process to evaluate and manage risk. The past practices of individual sites interpreting DOE policy and establishing local guidelines to conduct security analysis for risk determinations is in itself a risk to the effectiveness of the security program in that it lacks program integration. Analyses were not consistent from site to site and did not provide consistent application of DOE O 470.3C, *Design Basis Threat Policy (DBT)* or its successor (hereinafter referred to as DOE Threat Policy), security orders, tactical doctrine, or the Defense Intelligence Agency Nuclear Security Threat Capabilities Assessment (NSTCA) document. Inconsistencies resulted in an inability to compare relative risks across NNSA sites and hindered implementation of decisions affecting risk to the NNSA enterprise. To address this issue, DNS, working in conjunction with field office subject matter experts (SMEs) and nuclear security enterprise contractors, established a comprehensive program and standardized deliverables that support an efficient, effective, and sustainable risk management process.

5. REQUIREMENTS.

- a. Scoping Agreements: Scoping agreements must be used to identify the requirements and expectations for conducting an SRA or VA, which support the development of a site security plan (SSP) or individual security plan (SP). A VA must be used to evaluate the protection of protection level (PL) 1-4 assets and an SRA for PL 5-8 assets. The security contractor(s) and field office must develop scoping agreements using requirements outlined in NNSA Implementation Instructions (II) 470.4-2 Chapter 2 for VAs and Chapter 3 for SRAs.
- b. Asset Characterization: DOE assets must be identified and characterized to assign the appropriate PL and consequence value as a preliminary step to determine physical protection measures as defined in departmental directives. DOE assets must be characterized as defined in DOE policy and NNSA II 470.4-2 Chapter 1.
- c. Target Determination: Targets must be developed based on assets located at a facility. Selecting, screening, prioritizing, and the bounding of targets within and across PLs must be completed as described in NNSA II 470.4-2 Chapter 2 for VAs and Chapter 3 for SRAs.
- d. Radiological, Chemical, and Biological Sabotage Analysis: Sabotage analysis must be performed to ensure that appropriate controls are in place to prevent, mitigate, and respond to a potential attack commensurate with the hazard type. Sabotage analysis for each hazard type must follow the procedures stated in NNSA II 470.4-2 Chapter 1.
- e. Sabotage of Critical Infrastructure or Program Assets: Sabotage analysis must be performed to certify that appropriate controls are in place to prevent, mitigate, and

respond to a potential attack or loss of critical infrastructure assets or facilities. Analysis must be performed following the SRA process outlined in NNSA II 470.4-2 Chapter 3.

- f. Threat Characterization: Analysts must use the threats and objectives defined in the DOE Threat Policy and the process defined in NNSA II 470.4-2 to form the baseline for threat characterization. The complete range of DOE Threat Policy threats and their stated objectives must be analyzed as described in NNSA II 470.4-2 Chapter 2 for VAs and Chapter 3 for SRAs.
- g. Facility Characterization: The facility must be characterized to define performance relative to intrusion detection, access control, surveillance, alarm assessment, and barriers against a range of adversary tactics and threat types. Facility characterization forms the basis for pathway analysis and must be conducted using the parameters in NNSA II 470.4-2. Facility and transportation activities must be characterized as described in NNSA II 470.4-2 Chapter 2 for VAs and Chapter 3 for SRAs.
- h. Protective Force Characterization: The protective force (PF) must be characterized using the process outlined in NNSA II 470.4-2 Chapter 2 for VAs and Chapter 3 for SRAs. VA models used to characterize PF response must include performance testing data and Enterprise Mission Essential Task List (EMETL) program data. PF characterizations must include PF staffing and locations, PF equipment, and PF response to include: recapture, recovery, fresh pursuit, protective program defensive planning, as well as validation and verification of PF-related data.
- i. Application of the Insider: Insiders must be analyzed using the guidelines in NNSA II 470.4-2 Chapter 2 for VAs and Chapter 3 for SRAs. Analyses must include insider(s) acting alone and in collusion with an outside adversary.
- j. Scenario Development: The scenario development processes described in DOE Threat Policy and NNSA II 470.4-2 Chapters 2 and 3 must be used to develop scenarios to determine protection system effectiveness. Chapter 2 defines the methodology based on a distributed range of baseline scenarios and outlines the requirements for developing and modeling VA scenarios above and below baseline. Chapter 3 describes the scenario development process for SRAs.
- k. Neutralization Methodology: NNSA II 470.4-2 Chapter 2 must be used as the baseline to determine probability of neutralization. Probability of neutralization must be determined at each security layer of a facility using the NNSA standard set of modeling and simulation tools and effects databases. Data will be captured and documented to support the reported neutralization value as specifically outlined in NNSA II 470.4-2. EMETL results must be included in probability of neutralization calculations.

- l. Protection System Effectiveness Methodology: Protection system effectiveness (P_E) must be determined for each individual scenario that is developed. Analysts must determine distinct average P_E for targets within a storage facility, targets within a production facility, and targets in transport as described in the NNSA II 470.4-2. P_E for storage facilities, production facilities, and targets in transportation will not be combined to calculate a P_E average.
- m. Protection Strategy Change Analysis: Sites must analyze the effects to the changes in protection strategies or protection systems (upgrades or removals) using the processes detailed in NNSA II 470.4-2. Sites must base any Future-Years Nuclear Security Programming (FYNSP) or subsequent project requests and baseline changes on VA or SRA and include a cost/benefit analysis to support decisions.
- n. Quality Assurance: A quality assurance process must be established to verify the accuracy of the SRA or VA by conducting program reviews, validating the use of approved data sources and databases in the SRA or VA process, and by reviewing existing change control procedures to make sure changes to field security configurations do not occur without a supporting analytical basis. Field office personnel will confirm the SRA or VA conclusions are supported by accurate data sources and reasonable assumptions.
- o. Performance Assurance Program: An acceptable level of performance must be established and maintained to verify essential elements of a facility or site protection program are effective and functioning as designed, in accordance with the overall protection goals. Sites must adhere to the processes described in NNSA II 470.4-2 Chapter 5 for identifying essential elements and in the development of a Performance Assurance Program (PAP) plan.
- p. Site Security Plans (SSP) and Security Plans (SP)¹: All facilities and sites must have a consolidated SSP or individual SPs that reflect the assets, security interests, and approved Safeguards and Security (S&S) programs. The S&S programs must incorporate a risk-based approach and identify any residual risk. The risk-based approach identifies the consequences and residual risk associated with attempted theft, diversion, terrorist attack, industrial sabotage, radiological sabotage, chemical sabotage, biological sabotage, espionage, unauthorized access, compromise, and other acts as defined by DOE Threat Policy that may have an adverse effect on national security, the environment, or that pose a significant danger to DOE and NNSA federal and contractor employees or the public. An SRA or VA must be used to identify and communicate the security risk based on the protection elements in place or proposed to protect a departmental asset as prescribed in DOE Threat Policy. A single SRA or VA may be used to address multiple SPs provided the SRA or VA covers the assets identified in the plans. The SRA or VA assesses the likelihood that the security features in place can

¹ Security plans referenced in this document are those which apply to security asset protection and do not include other security plans such as those developed for foreign visits and assignments.

deliver the required effect to meet departmental standards and expectations. NNSA sites must adhere to the SRA and VA processes for identifying risks in SSPs or SPs outlined in DOE/NNSA policy, NNSA II 470.4-2 Chapter 2 for VAs and Chapter 3 for SRAs.

- q. Deviations from Policy: Equivalencies and exemptions from DOE protection requirements must be supported by an SRA or VA to facilitate an informed risk management decision. Sites must identify compensatory measures, if applicable, or alternative controls to be implemented within the supporting analysis. NNSA sites must adhere to the SRA process for deviations from policy outlined in NNSA II 470.4-2 Chapter 3 unless otherwise supported by an existing or new VA.
- r. Termination of Safeguards: A termination of safeguards request requires that designated facilities and nuclear materials for safeguards termination are assigned the proper categorization and attractiveness levels and the material is protected at the level identified and approved in the termination request. If the receiving facility meets DOE policy requirements for the material in question, no SRA is needed to support the request. If the receiving facility does not meet the physical protection requirements for the requested material, then an SRA must be conducted using the process identified in NNSA II 470.4-2 Chapter 3 to make certain that the material will be adequately protected, or risk is accepted at the appropriate level.
- s. Program Reviews: Program reviews must be accomplished using a working group comprised of the Office of Security Operations and Programmatic Planning (NA-71), DOE Office of Security (AU-50), local federal oversight, federal oversight from other NNSA sites, and field security risk SMEs. Program reviews are conducted at various stages of the VA process as identified in NNSA II 470.4-2 Chapter 6.
- t. Format and Content: NNSA sites must adhere to the NNSA methodologies and reporting formats in developing SRAs or VAs to support SSPs, SPs, exemptions/equivalencies, and termination of safeguards requests. The formats and required processes are detailed in NNSA II 470.4-2 Chapter 2 for VAs, Chapter 3 for SRAs, and Chapter 5 for PAPs. Sites must use NNSA II 470.4-2 as the single source to develop VAs and associated vulnerability assessment reports (VARs), develop SRAs, determine essential elements to support PAPs, and all other programs and processes listed in NNSA II 470.4-2. Any clarification or implementation procedures will be coordinated with DNS.
- u. Allocation of Resources: Sites must assign risk ratings/scores to recurring decrement or recurring over target security activities, projects, and procurements, within FYNSP budget requests in accordance with FYNSP guidance using the risk assessment processes identified in NNSA II 470.4-2 Chapters 2 and 3.
- v. Reporting Requirements and Modification: The E-SSPAP Program Manager will identify efficiencies and improvements working with field office oversight

representatives responsible for the planning and analysis program during annual field office reviews. The reviews will document recommendations to the Associate Administrator and Chief, DNS, for process improvements. The E-SSPAP Program Manager will incorporate changes and best practices into the annual update to the NNSA II 470.4-2.

6. RESPONSIBILITIES.

a. Administrator.

- (1) Approves exemptions from DOE security policy resulting in moderate risk.
- (2) Approves changes to security operations that do not require an exemption resulting in moderate risk.
- (3) Approves or delegates responsibilities for approving security conditions (SECON) plans to the Officially Designated Federal Security Authority (ODFSA).
- (4) Reviews exemptions from DOE security policy resulting in high risk, prior to sending to the Secretary.
- (5) Reviews changes to security operations that do not require an exemption resulting in high risk, prior to sending to the Secretary.

b. Associate Administrator and Chief, Defense Nuclear Security.

- (1) Approves E-SSPAP implementation instructions and field protocols in accordance with NNSA SD 470.4-1, *Defense Nuclear Security Federal Oversight Process*.
- (2) Approves termination of safeguards requests as prescribed by DOE/NNSA policy.
- (3) Approves low risk exemptions to DOE security policy.
- (4) Reviews E-SSPAP SD prior to sending to the Administrator.
- (5) Reviews equivalencies to DOE security policy prior to Field Office Manager (FOM) approval.
- (6) Reviews exemptions to DOE security policy that result in moderate and high risk, prior to sending to the Administrator and Secretary.

- (7) Reviews permanent changes to PF configuration and protection strategies impacting Field Security 20 (FS20) budget requirements prior to approval.
 - (8) Reviews permanent changes to physical security systems impacting FS20 budget requirements prior to approval.
 - (9) Assigns an E-SSPAP Program Manager to provide oversight of the E-SSPAP program.
- c. Director, Office of Security Operations and Programmatic Planning (NA-71).
- (1) Develops E-SSPAP SD and implementation instructions.
 - (2) Oversees implementation of E-SSPAP SD and implementation instructions.
 - (3) Reviews and provides recommendations on termination of safeguards as required by DOE/NNSA policy (requests must be supported by a VA or SRA as prescribed in NNSA II 470.4-2 Chapter 2 for VAs, and Chapter 3 for SRAs).
 - (4) Reviews and provides recommendations on PF Rules of Engagement along with NNSA General Counsel review.
 - (5) Reviews and provides recommendations for equivalencies prior to FOM approval (must be supported by a VA or SRA).
 - (6) Reviews and provides recommendations for exemptions prior to approval (must be supported by a VA or SRA).
 - (7) Conducts reviews of the following documentation provided by field offices²:
 - (a) Changes to site protection strategies that do not require a deviation from DOE policy resulting in low, moderate, or high security risk (must be supported by a VA or SRA);
 - (b) Vulnerability assessment reports (VARs);

² Reviews can occur through normal distribution of documents and NA-71 program reviews. Reviews do not indicate a need for concurrence prior to approval unless stated or required by existing policy. The program review process noted in the E-SSPAP SD will meet the review or consultation requirements for scoping agreements, VARs, and SRAs.

- (c) Permanent changes to PF configuration and protection strategy (must be supported by a VA or SRA);
 - (d) Permanent changes to physical protection systems configuration (must be supported by a VA or SRA);
 - (e) Security risk assessments;
 - (f) Performance assurance plans.
- d. Enterprise Safeguards and Security Planning and Analysis Program Manager.
 - (1) Implements the DNS E-SSPAP.
 - (2) Provides support to sites in implementing the E-SSPAP SD and other risk-related activities.
 - (3) Conducts program reviews to make sure the E-SSPAP is being implemented using the E-SSPAP SD guidelines.
 - (4) Conducts semi-annual E-SSPAP implementation panel working groups.
 - (5) Conducts annual updates to the E-SSPAP SD.
 - (6) Represents DNS on the Material Risk Review Committee (MRRC).
 - (7) Recommends the level of rigor and documentation required for an SRA to support security planning activities (documented in NNSA II 470.4-2).
 - (8) Partners with the ODFSA for recommendations to the site boundary distance used for purposes of radiological or chemical sabotage analysis to DNS (documented in the NNSA II 470.4-2).
 - (9) Recommends the grouping or bounding of assets for analysis purposes to DNS (documented in the NNSA II 470.4-2).
 - (10) Recommends the level of rigor and documentation required for roll-up analysis to DNS (documented in the NNSA II 470.4-2).
 - (11) Reviews and provides recommendations for deviations prior to approval and submittal to AU for consultation (must be supported by a VA or SRA).
- e. Field Office Manager.
 - (1) Approves SSPs supported by a VA or SRA.

- (2) Approves equivalencies to DOE security policy.
 - (3) Reviews changes to security operations that result in moderate or high risk.
 - (4) Reviews exemptions to DOE security policy resulting in low, moderate, or high risk.
- f. Officially Designated Federal Security Authority (Assistant Manager Safeguards and Security or other designated position).
- (1) Approves the scoping agreement for the conduct of a VA or SRA.
 - (2) Approves VARs or SRAs developed to support an SSP or SP.
 - (3) Approves SSPs and SPs supported by a VA or SRA.
 - (4) Approves pre-developed compensatory measures.
 - (5) Approves ad hoc compensatory measures.
 - (6) Approves SECON plans.
 - (7) Approves corrective action plans and closure to DOE Office of Enterprise Assessment (EA) findings.
 - (8) Approves PAP plans.
 - (9) Approves the PF Rules of Engagement.
 - (10) Approves permanent changes to PF and physical security systems configurations that do not require a deviation from DOE policy documented by a VA or SRA.
 - (11) Approves the PF fresh pursuit policy.
 - (12) Approves security incident response plans (SIRPs).
 - (13) Approves changes to security operations that do not require a deviation from DOE policy that result in low risk.
 - (14) Reviews SSPs supported by a VA or SRA prior to FOM signature.
 - (15) Reviews supplemental directives and implementation guidance.
 - (16) Reviews changes to security operations that do not require a deviation from DOE policy that result in moderate or high risk.

- (17) Reviews exemptions resulting in low, moderate, or high risk.
- (18) Reviews equivalencies prior to NA-71 review and AU-50 consultation.
- (19) Reviews termination of safeguards prior to sending to NA-71 for consultation.
- (20) Reviews efficiencies and improvements resulting from program reviews for applicability and feasibility of implementation.

g. Protection Program Management Oversight Manager.

- (1) Partners with the site contractor in the development of scoping agreements.
- (2) Provides oversight in all stages of the development of VAs and SRAs.
- (3) Partners with the E-SSPAP Program Manager in the development of E-SSPAP guidelines.
- (4) Represents the field office and participates in NNSA program reviews and Scenario Development Review Teams.

h. Officially Designated Security Authority (ODSA)/Site Security Contractor/Vulnerability Assessment Contractor.

- (1) Implements E-SSPAP SD.
- (2) Develops and presents SSPs and SPs.
- (3) Develops and presents changes to PF and physical security system configurations supported by a VA or SRA.
- (4) Develops and presents deviation requests.
- (5) Develops and presents pre-developed compensatory measures.
- (6) Develops and presents ad hoc compensatory measures.
- (7) Develops and presents SIRPs.
- (8) Develops and presents SECON plans.
- (9) Develops and presents corrective action plans and closures to findings as applicable.
- (10) Develops and presents PAPs.
- (11) Develops and presents the PF Rules of Engagement.

- (12) Develops and presents the PF firearms and ammunition configuration and procurement.
- (13) Develops and presents the scoping agreement and VAR.
- (14) Develops and presents scoping agreements and SRA(s).
- (15) Develops and presents permanent changes to security operations not requiring a deviation from DOE security policy (supported by a VA or SRA).
- (16) Develops and presents termination of safeguards.
- (17) Develops PF fresh pursuit plan and guidelines.

i. Heads of Field Elements.

- (1) Notify Contracting Officers (COs) of affected site/facility management contracts that must include the CRD.
- (2) Review procurement requests for new non-site/non-facility management contracts that involve classified information or nuclear materials and contain DEAR clause 952.204-2, *Security Requirements*.
- (3) If appropriate, notify the CO that the requirements of the CRD to the SD must be included in the contract.

j. Contracting Officers.

Incorporate the CRD of the SD and the Implementation Instructions into contracts in a timely manner upon notification of its applicability.

7. ACRONYMS. See Attachment 3

8. DEFINITIONS. Terms commonly used in the program are defined on the Office of Environment, Health, Safety and Security Policy Information Resource website, <https://pir.doe.gov/>.

9. REFERENCES. See Attachment 4.

10. CONTACT. Questions concerning this SD should be addressed to the Office of Defense Nuclear Security (NA-70) at (202) 586-8900.

BY ORDER OF THE ADMINISTRATOR:



Administrative Change Approved : 06-16-2021

Attachments:

1. Contractor Requirements Document
2. E-SSPAP SD Roles and Responsibilities Matrix
3. Acronyms
4. References

ATTACHMENT 1: CONTRACTOR REQUIREMENTS DOCUMENT

NNSA SD 470.4, ENTERPRISE SAFEGUARDS AND SECURITY PLANNING AND ANALYSIS PROGRAM (E-SSPAP)

This Contractor Requirements Document (CRD) establishes Enterprise Safeguards and Security Planning and Analysis Program (E-SSPAP) requirements for National Nuclear Security Administration (NNSA) contractors. Regardless of the performer of the work, the contractor is responsible for complying with the requirements of the CRD and flowing down CRD requirements to subcontractors at any tier.

This CRD is issued to identify requirements applicable to contractors. U.S. Department of Energy (DOE)/NNSA contractors must adhere to E-SSPAP program standards listed in the program elements of this document.

1. REQUIREMENTS.

- a. NNSA Implementation Instructions: The NNSA Implementation Instructions (II) 470.4-2 must be used as the standardized procedure for conducting security risk assessments (SRA) or vulnerability assessments (VA) and reporting risk within the NNSA nuclear security enterprise.
- b. Planning and Analysis Program: Programs must be developed using a consistent and standardized process. Programs associated with VAs, SRAs, performance assurance program (PAP) plans, and other safeguards and security documents listed in this CRD must be developed in accordance with and follow the process requirements in the NNSA II 470.4-2.
- c. Modeling Tools: Modeling and simulation tools used for the planning and analysis process must be approved and funded by the Office of Defense Nuclear Security.
- d. Scoping Agreements: Scoping agreements must be used to identify the requirements and expectations for conducting an SRA or VA that supports the development of a site security plan (SSP) or individual security plan (SP). A VA must support Protection Level (PL) 1-4 assets and an SRA for PL 5-8 assets. The security contractor(s) and field office must develop scoping agreements using requirements outlined in NNSA II 470.4-2 Chapter 2 for VAs and Chapter 3 for SRAs.
- e. Asset Characterization: DOE assets must be identified and characterized to assign the appropriate PL and consequence value as a preliminary step to determine physical protection measures as defined in departmental directives. DOE assets must be characterized as defined in DOE policy and NNSA II 470.4-2 Chapter 1.

- f. Target Determination: Targets must be developed based on assets located at a facility. Selecting, screening, prioritizing, and the bounding of targets within and across PLs must be completed as described in NNSA II 470.4-2 Chapter 2 for VAs and Chapter 5 for SRAs.
- g. Radiological, Chemical, and Biological Sabotage Analysis: Sabotage analysis must be performed to confirm that appropriate controls are in place to prevent, mitigate, and respond to a potential attack commensurate with the type of hazard. Sabotage analysis for each type of hazard must follow the procedures stated in NNSA II 470.4-2 Chapters 1, 2, and 3.
- h. Sabotage of Critical Infrastructure or Program Assets: Sabotage analysis must be performed to verify that appropriate controls are in place to prevent, mitigate, and respond to a potential attack or loss of critical infrastructure assets or facilities. Analysis must be performed following the SRA process outlined in NNSA II 470.4-2 Chapter 3.
- i. Threat Characterization: Analysts must use the threats and objectives defined in DOE Order 470.3C, *Design Basis Threat Policy (DBT)* or its successor (hereinafter referred to as DOE Threat Policy) and the process defined in NNSA II 470.4-2 to form the baseline for threat characterization. The complete range of DOE Threat Policy threats and their stated objectives must be analyzed as described in NNSA II 470.4-2 Chapter 2 for VAs and Chapter 3 for SRAs.
- j. Facility Characterization: The facility must be characterized to define performance relative to intrusion detection, access control, surveillance, alarm assessment, and barriers against a range of adversary tactics and threat types. Facility characterization forms the basis for pathway analysis and must be conducted using the parameters in NNSA II 470.4-2. Facility and transportation activities must be characterized as described in NNSA II 470.4-2 Chapter 2 for VAs and Chapter 3 for SRAs.
- k. Protective Force Characterization: The protective force (PF) must be characterized using the process outlined in NNSA II 470.4-2. VA models used to characterize PF response must include performance testing data and Enterprise Mission Essential Task List (EMETL) program data. PF characterizations must include PF staffing and locations, PF equipment, and PF response to include: recapture, recovery, fresh pursuit, protective program defensive planning, as well as validation and verification of PF-related data.
- l. Application of the Insider: Insiders must be analyzed using the guidelines in NNSA II 470.4-2 Chapter 2 for VAs and Chapter 3 for SRAs. Analyses must include insider(s) acting alone and in collusion with an outside adversary as applicable based on the DOE Threat Policy.
- m. Scenario Development: The scenario development processes described in the DOE Threat Policy and NNSA II 470.4-2 must be used to develop scenarios to

determine protection system effectiveness. NNSA II 470.4-2 Chapter 2 defines the methodology based on a distributed range of baseline scenarios and outlines the requirements for developing and modeling VA scenarios above and below baseline. NNSA II 470.4-2 Chapter 3 describes the scenario development process for SRAs.

- n. Neutralization Methodology: NNSA II 470.4-2 Chapter 2 must be used as the baseline to determine probability of neutralization. Probability of neutralization must be determined at each security layer of a facility using the NNSA standard set of modeling and simulation tools and effects databases. Data will be captured and documented to support the reported neutralization value as specifically outlined in the NNSA II 470.4-2. EMETL results must be included in probability of neutralization calculations.
- o. Protection System Effectiveness Methodology: Protection system effectiveness (P_E) must be determined for each individual scenario that is developed. Analysts must determine distinct average P_E for targets within a storage facility, targets within a production facility, and targets in transport as described in NNSA II 470.4-2. P_E for storage facilities, production facilities, and targets in transport will not be combined to calculate a P_E average.
- p. Protection Strategy Change Analysis: Sites must analyze the effects to changes in protection strategies or protection systems (upgrades or removals) using the processes detailed in NNSA II 470.4-2. Sites must base any Future-Years Nuclear Security Programming (FYNSP) or subsequent project requests and baseline changes on vulnerability assessments or security risk assessments and include a cost/benefit analysis to support decisions.
- q. Quality Assurance: A quality assurance process must be established to verify the accuracy of the SRA or VA by conducting programmatic reviews, validating the use of approved data sources and databases in the SRA or VA process, and by reviewing existing change control procedures to make sure changes to field security configurations do not occur without a supporting analytical basis. Field office personnel will confirm the SRA or VA conclusions are supported by accurate data sources and reasonable assumptions.
- r. Performance Assurance Program: An acceptable level of performance must be established and maintained to verify essential elements of a facility or site protection program are effective and functioning as designed, in accordance with the overall protection goals. Sites must adhere to the process identified in NNSA II 470.4-2 Chapter 5 for identifying essential elements and in the development of a Performance Assurance Program (PAP) plan.

- s. Site Security Plans and Security Plans³: All facilities and sites must have a consolidated SSP or individual SPs that reflect the assets, security interests, and approved safeguards and security (S&S) programs. The S&S programs must incorporate a risk-based approach and identify any residual risk. The risk-based approach must protect against the consequences of attempted theft, diversion, terrorist attack, industrial sabotage, radiological sabotage, chemical sabotage, biological sabotage, espionage, unauthorized access, compromise, and other acts that may have an adverse effect on national security, the environment, or that pose a significant danger to DOE and NNSA federal and contractor employees or the public. An SRA or VA must be used to identify and communicate the security risk based on the protection elements in place or proposed to protect a departmental asset. A single SRA or VA may be used to address multiple SPs provided the SRA or VA covers the assets identified in the plans. The SRA or VA assesses the likelihood that the security features in place can deliver the required effect to meet departmental standards and expectations. NNSA sites must adhere to the SRA and VA process for identifying risks in SPs outlined in DOE/NNSA policy, NNSA II 470.4-2 Chapter 2 for VAs, and Chapter 3 for SRAs.
- t. Deviations from Policy: Equivalencies and exemptions from DOE protection requirements must be supported by an SRA or VA to facilitate an informed risk management decision. Sites must identify compensatory measures, if applicable, or alternative controls to be implemented. NNSA sites must adhere to the SRA process for deviations from policy outlined in NNSA II 470.4-2 Chapter 3 unless otherwise supported by an existing or new VA.
- u. Termination of Safeguards: A termination of safeguards request requires that designated facilities and nuclear materials for safeguards termination are assigned the proper categorization and attractiveness levels and the material is protected at the level identified and approved in the termination request. If the receiving facility meets DOE policy requirements for the material in question, no SRA is needed to support the request. If the receiving facility does not meet the physical protection requirements for the requested material, then an SRA must be conducted using the process identified in NNSA II 470.4-2 Chapter 3 to make sure that the material will be adequately protected, or risk is accepted at the appropriate level.
- v. Program Reviews: Program reviews must be accomplished using a working group comprised of the Office of Security Operations and Programmatic Planning (NA-71), DOE Office of Security (AU-50), local federal oversight, federal oversight from other NNSA sites, and field security risk SMEs. Program reviews are conducted at various stages of the VA process as identified in NNSA II 470.4-2 Chapter 6.

³ Security plans referenced in this document are those which apply to security asset protection and do not include other security plans such as those developed for foreign visits and assignments.

- w. Format and Content: NNSA sites must adhere to the NNSA methodologies and reporting formats in developing SRAs or VAs to support SSPs, SPs, exemptions/equivalencies, and termination of safeguards requests. The formats and required processes are detailed in NNSA II 470.4-2 Chapter 2 for VAs, Chapter 3 for SRAs, and Chapter 5 for PAPs. Sites must use NNSA II 470.4-2 as the single source to develop VAs and associated vulnerability assessment reports (VARs), develop SRAs, determine essential elements to support PAPs, and all other programs and processes listed in this Supplemental Directive (SD). Any clarification or implementation procedures will be coordinated with Defense Nuclear Security (DNS).
 - x. Allocation of Resources: Sites must assign risk ratings or scores to recurring decrement or recurring over target activities, projects, and procurements, within FYNSP budget requests in accordance with the risk assessment process identified in NNSA II 470.4-2 Chapters 2 and 3.
 - y. Reporting Requirements and Modification: The E-SSPAP Program Manager must identify efficiencies and improvements working with field office oversight representatives responsible for security risk management during annual field office reviews. The reviews will document recommendations to the Associate Administrator and Chief, Defense Nuclear Security (CDNS) for process improvements. The E-SSPAP Program Manager will incorporate changes and best practices into the annual update to the NNSA II 470.4-2. The E-SSPAP Program Manager will generate an annual report documenting the status of security across the nuclear security enterprise.
2. RESPONSIBILITIES. Roles and responsibilities outlined in Attachment 2 of this document must be used for the E-SSPAP document review and approval process.
- a. Field Office Manager (FOM).
 - (1) Approves SSPs supported by a VA or SRA.
 - (2) Approves equivalencies to DOE security policy.
 - (3) Reviews changes to security operations that result in moderate or high risk.
 - (4) Reviews exemptions to DOE security policy resulting in low, moderate, or high risk.
 - b. Officially Designated Federal Security Authority (Assistant Manager Safeguards and Security or other designated position).
 - (1) Approves the scoping agreement for the conduct of a VA or SRA.
 - (2) Approves VARs or SRAs developed to support an SSP or SP.

- (3) Approves SPs supported by a VA or SRA.
- (4) Approves pre-developed compensatory measures.
- (5) Approves ad hoc compensatory measures.
- (6) Approves SECON plans.
- (7) Approves corrective action plans and closures to enterprise assessment findings.
- (8) Approves PAP plans.
- (9) Approves the PF Rules of Engagement.
- (10) Approves permanent changes to PF and physical security systems configurations that do not require a deviation from DOE policy documented by a VA or SRA.
- (11) Approves the PF fresh pursuit policy.
- (12) Approves PF firearm ammunitions configuration and procurement.
- (13) Approves security incident response plans (SIRPs).
- (14) Approves changes to security operations that do not require a deviation from DOE policy and result in low risk.
- (15) Reviews SSPs supported by a VA or SRA prior to FOM signature.
- (16) Reviews supplemental directives and implementation instructions.
- (17) Reviews changes to security operations that do not require a deviation from DOE policy resulting in moderate or high risk.
- (18) Reviews exemptions resulting in low, moderate, or high risk.
- (19) Reviews equivalencies prior to NA-71 review and AU-50 consultation.
- (20) Reviews termination of safeguards prior to sending to NA-71 for consultation.

c. Protection Program Management Oversight Manager.

- (1) Partners with the site contractor in the development of scoping agreements.
- (2) Provides oversight in all stages of the development of VAs and SRAs.

- (3) Partners with the E-SSPAP Program Manager in the development of E-SSPAP guidelines.
 - (4) Represents the field office and participates during the NNSA program reviews and in the Scenario Development Review Team.
- d. Officially Designated Security Authority (ODSA)/Site Security Contractor/Vulnerability Assessment Contractor.
- (1) Implements E-SSPAP SD.
 - (2) Develops and presents SSPs and SPs.
 - (3) Develops and presents changes to PF and physical security system configurations supported by a VA or SRA.
 - (4) Develops and presents deviation requests.
 - (5) Develops and presents pre-developed compensatory measures.
 - (6) Develops and presents ad hoc compensatory measures.
 - (7) Develops and presents SIRPs.
 - (8) Develops and presents SECON plans.
 - (9) Develops and presents corrective action plans and closures to findings as applicable.
 - (10) Develops and presents PAP plans.
 - (11) Develops and presents the PF Rules of Engagement.
 - (12) Develops and presents the PF firearms and ammunition configuration and procurement.
 - (13) Develops and presents the scoping agreement and VAR.
 - (14) Develops and presents scoping agreements and SRA(s).
 - (15) Develops and presents permanent changes to security operations not requiring a deviation from DOE policy (supported by a VA or SRA).
 - (16) Develops and presents termination of safeguards.
 - (17) Develops PF fresh pursuit plan and guidelines.

3. DEFINITIONS. Terms commonly used in the program are defined on the Office of Environment, Health, Safety and Security Policy Information Resource website, <https://pir.doe.gov/>.

ATTACHMENT 2. ENTERPRISE SAFEGUARDS AND SECURITY PLANNING AND ANALYSIS PROGRAM (E-SSPAP) SUPPLEMENTAL DIRECTIVE ROLES AND RESPONSIBILITIES MATRIX

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

The following table is intended to provide a responsibility matrix for various Safeguards and Security risk-related documents. Risk acceptance authorities outlined in DOE policy apply. Reviews (as stated above and in the table below) can occur through normal distribution of documents, scheduled peer reviews, and NA-71 program reviews. Reviews do not indicate a need for concurrence prior to approval unless required by existing policy.

The program review process noted in NNSA Implementation Instructions 470.4-2 will meet the review or consultation requirements for scoping agreements, vulnerability assessment reports, and security risk assessments.

Document/Plan	Develop	Review and/or Consultation		Approve	Copy
		Reviewing Org(s)	Prior to Approval		
High Risk Exemptions to Security Policy (supported by a VA or SRA)	ODSA or Contractor	ODFSA	X	S-1	N/A
		FOM	X		
		NA-71	X		
		CDNS	X		
		NA-1	X		
Security Risk Documentation for Changes in Security Operations Resulting in High Risk (not requiring a deviation from policy)	ODSA or Contractor	ODFSA	X	S-1	N/A
		FOM	X		
		NA-71	X		
		CDNS	X		
		NA-1	X		
Supplemental Directives	NA-71	ODFSA	X	NA-1	FOM ODFSA ODSA
		AU-50	X		
		CDNS	X		
Moderate Risk Exemptions to Security Policy (supported by a VA or SRA)	ODSA or Contractor	ODFSA	X	NA-1	N/A
		FOM	X		
		NA-71	X		
		CDNS	X		

Document/Plan	Develop	Review and/or Consultation		Approve	Copy
		Reviewing Org(s)	Prior to Approval		
Security Risk Documentation for Changes in Security Operations resulting in Moderate Risk (not requiring a deviation from policy)	ODSA or Contractor	ODFSA	X	NA-1	N/A
		FOM	X		
		NA-71	X		
		CDNS	X		
Low Risk Exemptions to Security Policy (supported by a VA or SRA)	ODSA or Contractor	ODFSA	X	CDNS	N/A
		FOM	X		
		NA-71	X		
		AU-50	X		
Implementation Guidance (e.g., Annual Implementation Instruction updates)	NA-71	ODFSA	X	CDNS	FOM ODFSA ODSA
Termination of Safeguards	ODSA or Contractor	ODFSA	X	CDNS	N/A
		NA-71	X		
		AU-50	X		
Equivalency to Security Policy (supported by a VA or SRA)	ODSA or Contractor	ODFSA	X	FOM	N/A
		NA-71	X		
		CDNS	X		
		AU-50	X		
Site Security Plan(s) - supported by VA(s) and/or SRA(s)	ODSA or Contractor	ODFSA	X	FOM	NA-71
SRAs Supporting a Site Security Plan	ODSA or Contractor	NA-71	Not Required ⁵	ODFSA	NA-71
Vulnerability Assessment Reports	ODSA or Contractor	NA-71	Not Required ⁵	ODFSA	NA-71
Corrective Action Plans (CAP): Enterprise Assessment (EA) Findings	ODSA or Contractor ODFSA	N/A	Not Required	ODFSA	Notify NA-71 (SSIMS)

⁵ Program review process fulfills the review requirement for NA-71.

Document/Plan	Develop	Review and/or Consultation		Approve	Copy
		Reviewing Org(s)	Prior to Approval		
Closure of Safeguards & Security EA Findings	ODSA or Contractor	N/A	Not Required	ODFSA	Notify NA-71 (SSIMS)
Performance Assurance Program (PAP) Plans	ODSA or Contractor	NA-71	Not Required ⁵	ODFSA	N/A
Security Risk Documentation for Low Risk Changes in Security Operations (not requiring a deviation from policy)	ODSA or Contractor	NA-71	Not Required	ODFSA	N/A
Protective Force Fresh Pursuit Policy	ODSA or Contractor	N/A	Not Required	ODFSA	N/A
Protective Force Rules of Engagement	ODSA or Contractor	NA-71	Not Required	ODFSA	N/A
		NNSA GC	Not Required		
Scoping Agreements	ODSA or Contractor	NA-71	Not Required ⁵	ODFSA	N/A
Security Incident Response Plans (SIRPs)	ODSA or Contractor	N/A	Not Required	ODFSA	N/A
Predeveloped Compensatory Measures	ODSA or Contractor	N/A	Not Required	ODFSA	N/A
Ad hoc Compensatory Measures	ODSA or Contractor	N/A	Not Required	ODFSA	N/A
Security Conditions (SECON) Plans	ODSA or Contractor	N/A	Not Required	ODFSA	N/A
Permanent changes to Protective Force Configuration not requiring a deviation	ODSA or Contractor	NA-71	X ⁶	ODFSA	N/A
		CDNS	X	ODFSA	N/A
Permanent changes to Physical Security System (PSS) not requiring a deviation	ODSA or Contractor	NA-71	X ⁶	ODFSA	N/A
		CDNS	X	ODFSA	N/A
Protective Force firearms and ammunition configuration and procurement	ODSA or Contractor	N/A	Not Required	ODFSA	N/A

⁵ Program review process fulfills the review requirement for NA-71.

⁶ Review required before approval for changes impacting FS-20 budget requirements.

THIS PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT 3: ACRONYMS

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

- a. AMSS: Assistant Manager Safeguards and Security
- b. CDNS: Chief, Defense Nuclear Security
- c. CRD: Contractor Requirements Document
- d. DNS: Defense Nuclear Security
- e. DOE: Department of Energy
- f. DOT: Department of Transportation
- g. E-SSPAP: Enterprise Safeguards and Security Planning and Analysis Program
- h. FOM: Field Office Manager
- i. FS20: Field Security 20
- j. FYNISP: Future-Years Nuclear Security Programming
- k. M&O: Management & Operating
- l. NNSA: National Nuclear Security Administration
- m. ODFSA: Officially Designated Federal Security Authority
- n. ODSA: Officially Designated Security Authority
- o. OUO: Official Use Only
- p. PAP: Performance Assurance Program
- q. PE: Protection System Effectiveness
- r. PF: Protective Force
- s. PL: Protection Level
- t. S&S: Safeguards and Security
- u. SD: Supplemental Directive
- v. SIRP: Security Incident Response Plan
- w. SME: Subject Matter Expert

- x. SP: Security Plan
- y. SRA: Security Risk Assessment
- z. SSP: Site Security Plan
- aa. VA: Vulnerability Assessment
- bb. VAR: Vulnerability Assessment Report

ATTACHMENT 4: REFERENCES

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

- a. NNSA SD 470.4-2 Implementation Instructions, Dated March 2020
- b. DOE Order 470.3C Change 1, *Design Basis Threat (DBT) Order*, dated 9-9-20
- c. DOE Order 470.4B Chg 2 (MinChg), *Safeguards and Security Program*, dated 1-17-17
- d. DOE Order 473.3A, *Protection Program Operations*, dated 3-23-16
- e. NNSA SD 470.4-1, *Defense Nuclear Security Federal Oversight Process*, dated 4-1-16