SUPPLEMENTAL DIRECTIVE

NNSA SD 470.4-1

Approved: 4-1-16

DEFENSE NUCLEAR SECURITY FEDERAL OVERSIGHT PROCESS

NATIONAL NUCLEAR SECURITY ADMINISTRATION
Office of Defense Nuclear Security

**OFFICE OF PRIMARY INTEREST (OPI):
Office of Defense Nuclear Security**

THIS PAGE INTENTIONALLY LEFT BLANK

DEFENSE NUCLEAR SECURITY FEDERAL OVERSIGHT PROCESS

1. PURPOSE. This National Nuclear Security Administration (NNSA) Supplemental Directive (SD) prescribes the *Defense Nuclear Security (DNS) Federal Oversight Process*.

   This SD provides information for the execution of the *DNS Federal Oversight Process*. This process establishes formality of operations and provides information to facilitate effective decision-making concerning security operations, policies, and resources for the nuclear security enterprise (NSE).

   Effective Federal oversight is paramount for the security mission. This SD provides the framework necessary to describe existing security processes to include complementary oversight, assistance, and communication mechanisms. It enhances identification of gaps and areas of inconsistency, and supports the development of measures to correct or mitigate deficiencies and minimize inefficiencies. DNS will employ and rely on the full spectrum of activities described herein to achieve that end.

2. CANCELLATION. None.

3. APPLICABILITY.

   a. Federal. This SD applies to NNSA elements (i.e., DNS and NNSA Field Offices). This SD automatically applies to NNSA elements created after it is issued.

   b. Contractors. This SD does not apply to contractors.

   c. Equivalencies.

      (1) In accordance with the responsibilities and authorities assigned by Executive Order 12344, codified at 50 USC sections 2406 and 2511 and to ensure consistency through the joint Navy/DOE Naval Nuclear Propulsion Program, the Deputy Administrator for Naval Reactors (Director) will implement and oversee requirements and practices pertaining to this Directive for activities under the Director's cognizance, as deemed appropriate.

      (2) The Kansas City National Security Campus will use applicable national standards and requirements for execution of the S&S program.

4. BACKGROUND. All safeguards and security (S&S) programs, practices, and procedures developed within NNSA must be consistent with the Department of Energy (DOE) requirements and all national requirements (e.g., Atomic Energy Act of 1954, Executive Orders, U.S. Code, Code of Federal Regulations, etc.).

5. REQUIREMENTS. This SD is a document that centralizes the Federal oversight process and formalizes monitoring of the NNSA contractor performance at fixed sites. It will be

re-evaluated and revised annually, as appropriate. Additional information is included in Appendixes 1-3 of this SD.

a. Operational Awareness. Appendix 1 outlines awareness activities and provides requirements for the use of numerous data sources and activities in order to support the oversight process and track implementation of the S&S programs. This appendix addresses data analysis and tracking of information in partnership with the Field Offices as a means to prioritize and focus on areas either at a site or across the NSE.

b. Security Reviews and Technical Assistance. Appendix 2 addresses requirements for conducting oversight security reviews and technical assistance support in partnership with the Field Offices. These oversight activities are designed to assist Field Offices and strengthen Headquarters' understanding of field security operations and issues.

c. DNS and Field Office Communications. Appendix 3 identifies requirements for communication mechanisms in the notification and oversight process of S&S issues or areas of concern.

5. RESPONSIBILITIES.

a. Chief of Defense Nuclear Security (CDNS)/Associate Administrator for Defense Nuclear Security:

1) Serve as the NNSA Officially Designated Federal Security Authority (ODFSA) responsible for the development and implementation of S&S programs and operations for NNSA security organizations.

2) Lead the NNSA Cognizant Security Office.

3) Provide programmatic guidance, direction, and program oversight to measure effective development and implementation of S&S programs and operations for NNSA sites.

4) Develop implementing guidance and standards related to the NNSA S&S Program. Ensure information is clear, consistent, and uniformly applied.

5) Review site-level exemption and equivalency requests submitted by Field Offices. Ensure all formal requests describe any increase in security risks and proposed mitigation measures with submissions.

6) Develop and allocate the security budget to support DNS mission.

7) Set strategic vision and multiyear objectives for the nuclear security programs.

8) Provide subject matter experts (SMEs) to support field requests for assistance in functional areas.

b. Field Office Managers/Assistant Managers for Safeguards and Security (AMSS):

1) Delegated ODFSA responsibility for security program plans and activities at their specific sites. This authority can be further delegated to the site's Assistant Manager for Safeguards and Security.

2) Designated as Cognizant Security Offices for facilities under their line management authority.[1]

3) Identify Federal roles, responsibilities, and authorities necessary to direct, guide, and oversee security operations at their respective site.

4) Ensure the effective protection of NNSA critical assets through security plan approvals, risk management decisions, and program management activities.

5) Ensure security requirements and performance expectations are captured in NNSA contracts.

6) Direct contractors to implement S&S programs through the Contracting Officer or Contracting Officer Representative authority.

7) Conduct operational awareness activities that are sufficient to support quarterly submission of the consolidated annual operating plan report to DNS, and to provide the basis for Corporate Performance Evaluation Process (CPEP) ratings.

8) Review and validate, as appropriate, the NNSA site's deliverables such as budget requests, annual operating plan reports, and other reports before submitting to DNS.

9) Determine site Future Years Nuclear Security Program (FYNSP) budget requirements, and submit the budget requests to DNS.

10) Report incidents of security concern (IOSC) to DNS in accordance with established security requirements and report relevant security concerns to the Emergency Operations Center at headquarters.

11) Ensure Federal surveys and contractor self-assessments evaluate all S&S topical and sub-topical areas relating to Program Management Operations, Physical Protection, Protective Force, Information Protection, Personnel

[1] The CDNS can delegate Cognizant Security Office responsibilities down to the NNSA Field Offices.

Security, and Material Control and Accountability that are applicable at the facility or site being surveyed. Conduct oversight and operational awareness activities sufficient to support an annual comprehensive evaluation of S&S program performance.

12) Establish and maintain an annual schedule for conducting Federal surveys and other activities for oversight of contractors. Ensure Federal surveys and contractor self-assessments are conducted on Category I special nuclear material (SNM) facilities with security functions directly supporting protection of nuclear materials, at a minimum, once every 12 months, except when formally extended by the CDNS. Determine frequency of Federal surveys at non-Category I SNM facilities consistent with the site's risk management principles. Ensure contractors at non-Category I SNM facilities conduct an annual self-assessment.

NOTE: The following criteria must be met prior to CDNS formal approval of a Federal survey extension. The facility must be rated as "Satisfactory" during the most recent Office of Enterprise Assessments inspection; the facility has no unmitigated deficiencies or risks that impact the security posture and topical area ratings are at least "Satisfactory" from the previous Federal survey of the contractor; and, topical area ratings from the most recent contractor self-assessment must have a minimal rating of "Satisfactory."

13) Ensure formal reports are prepared for Federal surveys and contractor self-assessments to include findings (refer to Appendix 4, Field Security Survey and Self-Assessment Report Content for an example). Ensure all findings have corrective action plans and are tracked until closure of deficiencies.

14) Ensure corrective actions for findings identified during surveys and self-assessments are implemented in a timely and effective manner, and validate the effectiveness of corrective actions to prevent recurrence of issues.

c. <u>DNS Security Operations and Programmatic Planning (NA-71) Program Managers:</u>

1) Plan and implement security activities as assigned under their specific topical area in accordance with the mission and goals of DNS.

2) Assist in development of initiatives to support the strategic direction of nuclear security programs.

3) Develop and implement topical area program with goals and objectives for an effective S&S program.

4) Lead core team development of the annual budget and operating plan review in support of the overall S&S program.

5) Assist desk officer as needed in executing the program evaluation framework to assess strengths of the S&S program and to identify opportunities for improvement.

d. DNS Desk Officers:

1) Perform as a Headquarters-based DNS advocate for supporting the Field Office's oversight requirements and needs.[2]

2) Assist in performing security activities as assigned in accordance with mission and goals of DNS.

3) Perform responsibilities as the CPEP representative.

4) Coordinate, collect, and maintain all required S&S information regarding their assigned Field Office to ensure materials are relevant and current (e.g., security plans, assessments, findings, deviations, etc.).

5) Monitor all evaluations, inspections, and surveys to include associated corrective actions.

6) Serve as the point of contact to coordinate actions with the respective NA-71 program managers.

7) Provide status updates to DNS leadership concerning site security issues.

8) Review formal incoming and outgoing correspondence pertaining to respective site.

9) Provide periodic updates to Field Offices on DNS activities related to the sites.

10) Conduct site visits and interacts with the AMSS and S&S staff.

11) Monitor updates concerning site-specific issues requiring CDNS action.

6. REFERENCES.

a. DOE Policy 226.1B, *Department of Energy Oversight Policy*

b. DOE Order 226.1B, *Implementation of Department of Energy Oversight Policy*

[2] Each NNSA site will have a Federal DNS lead designated as a desk officer, responsible for the above listed performance and administrative matters. All management decision-making will continue to be provided by DNS leadership, with the respective desk officer being notified for situational awareness purposes. The desk officer position is not intended to eliminate or hinder the Field Office's engagement or interaction with the CDNS, Deputy Associate Administrator for DNS, or DNS SMEs.

c. DOE Guide 226.1-2A*, Federal Line Management Oversight of Department of Energy Nuclear Facilities*

d. DOE Order 470.4B, *Safeguards and Security Program*

e. DOE Order 473.3, *Protection Program Operations*

f. NAP-21, *Transformational Governance and Oversight*

g. *DNS Evaluation and Performance Assurance Plan*

h. DNS Standard Operating Procedure/SOP-13-11, *DNS Corporate Performance Evaluation Process*

i. *DNS Safeguards & Security Planning, Programming, Budgeting and Evaluation Plan*

7. 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/

8. 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:

Frank G. Klotz

Frank G. Klotz
Administrator

Appendixes
1. Operational Awareness
2. Security Reviews and Technical Assistance
3. DNS and Field Office Communications
4. Field Security Survey and Self-Assessment Report Content
5. Request for Program Office Support Form
6. DNS Security Review Plan Content
7. DNS Security Review Report Content
8. NNSA Event Notification Matrix

APPENDIX 1: OPERATIONAL AWARENESS

1. Operational awareness activities increase confidence that S&S operations are effectively performed and provide early identification of vulnerabilities and deficiencies. These activities include maintaining current awareness of the conditions and issues that could affect operations; performance expectations and measures; and, contract deliverables and requirements. The specific components of operational awareness are designed to provide data and ensure information is reported, analyzed, and understood in a manner that communicates the health of S&S programs.

2. DNS operational awareness requires lines of communication among stakeholders (i.e., Headquarters, Field Offices, and contractors). In conducting operational awareness activities and oversight of the S&S mission, DNS and Field Offices will rely on data collection, analysis, and tracking sources. These deliverables and activities will help DNS anticipate shortfalls and focus resources, as well as identify risk and determine if assistance is needed in the field. Best practice processes and activities will also be captured as a benchmark and disseminated throughout the NSE for consideration at NNSA sites.

   a. <u>Data Collection, Analysis, and Tracking</u>.

      1) Collecting, analyzing, and tracking information are important steps in understanding site-specific and NSE-wide S&S performance. One of the objectives of DNS situational awareness activities is to understand performance challenges, as well as establish priorities and processes for the NSE to address issues. Understanding problem areas will enable DNS, in partnership with the Field Offices, to prioritize and focus on areas requiring attention either at a site or across the NSE. DNS collects information from several existing sources including, but not be limited to:

         a) Office of Enterprise Assessments (EA) reports;

         b) DNS Technical Assistance Activities and Site Assistance Visits;

         c) Field Office and contractor self-assessment reports;

         d) Field Office surveys of contractor S&S performance;

         e) Internal and external government reports (Government Accountability Office, Office of Inspector General, etc.);

         f) Safeguards and Security Information Management System (SSIMS) database[3];

[3] SSIMS is the official DOE database for tracking inspections, surveys, findings, corrective action plans, incidents of security concern, deviations, and facility data and approval records.

g) Site Annual Operating Plans (AOP);

h) Protective Force Supplemental and Physical Security Systems Supplemental reports;

i) Protective Force Enterprise Mission Essential Task List (EMETL) self-assessment reports;

j) Exemptions and Equivalencies;

k) Conference calls and face-to-face meetings;

l) NA-71/AMSS bi-weekly teleconferences and periodic meetings;

m) CPEP reports; and,

n) DNS S&S Special Emphasis and Programmatic Reviews.

2) DNS will analyze and track information to identify potential concerns and best practices at individual sites and across the NSE. DNS analysis and tracking will facilitate the identification of security gaps and development of performance standards/expectations for the NSE. The evaluation of information will also be provided to the DNS leadership and Field Offices for their use in addressing those areas requiring additional attention with the level of effort (e.g., manpower and funding) needed for S&S success. This information is archived in the SharePoint site (Federal Field Offices and Headquarters security staff, as well as the NA-71 support staff have access) to ensure transparency and strengthen communication between the Field Offices and DNS.

3) These documents and activities are analyzed by SMEs, who extract data to identify potential issues requiring management attention. This analysis will also include a review of the findings, observations, opportunities for improvement, and identification of causal factors, where possible. DNS has access to all information listed above in section 2.a.1 with the exception of Field Office and contractor self-assessments and contractor survey reports. Field Offices must provide these documents to their assigned desk officer upon final completion.

4) The Field Office deliverables or field activities may trigger a special emphasis review. A special emphasis review could be initiated for several reasons, such as loss of Protective Force weapons, security incidents involving special access programs, or unauthorized access to a security area. The CDNS may initiate a special emphasis review for any area or activity that is not performing to expected standards or when NNSA management determines that an independent review is appropriate.

5) Data analysis is conducted in conjunction with the CPEP Program and under the overall direction of the CDNS. NA-71 SMEs and DNS budget analysts are required to complete their examination of the information contained in submitted site reports, and update the NA-71 SharePoint site within 30 calendar days of receiving source documents. Results of the analyses are communicated to NNSA/DNS leadership, Field Offices, and NA-71 staff by various means to include:

a) DNS and AMSS meetings;

b) Bi-weekly NA-71 and AMSS teleconferences;

c) Individual teleconferences with the Field Office AMSSs;

d) Written CPEP reports with NNSA leadership and Field Office AMSSs;

e) DNS leadership CPEP meetings; and,

f) NA-71 SharePoint site.

b. Performance Objectives and Criteria.

1) To understand the overall health and status of S&S programs at each site, it is important to evaluate S&S performance through a system of well-defined objectives that are reported uniformly across the NSE. DNS partners with the Field Offices to identify, communicate, and monitor progress of key priorities for the year. DNS uses the site's AOP to track budget spend rates, which are submitted in an established format, updated quarterly, and reviewed by DNS SMEs. Field Offices will provide AOPs, Protective Force Supplemental reports (i.e., budget, staffing, attrition rate, labor hours, etc.) and Physical Security Systems Supplemental reports (i.e., budget, staffing, site deployed assets, alarm rates, etc.). These reports are due within 21 calendar days following the last day of each respective quarter (i.e., December, March, June, and September).

2) DNS evaluates oversight submissions from the Field Offices and analyzes performance for the fiscal year against established criteria and objectives. DNS will send any questions or issues back to the sites for clarification. The analysis is documented and recommendations are provided to DNS leadership for decisions and planning.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX 2: SECURITY REVIEWS AND TECHNICAL ASSISTANCE

1. DNS will conduct security reviews and technical assistance activities in partnership with the Field Offices. These activities are designed to assist Field Offices and strengthen Headquarters' understanding of field security operations, as well as identify possible issues and best practices. Additionally, these activities will assist DNS in evaluating S&S activities for standardization and determine if there are common issues across the NSE.

2. DNS will assist in Field Office activities through on-site or virtual support with emphasis on strengthening oversight and monitoring of contractor performance assurance and self-assessment functions. DNS staff may augment the Field Office survey and/or self-assessment teams to fulfill oversight responsibilities at the request of the Field Office Manager or AMSS. The following are the primary types of oversight and support activities:

   a. Technical Assistance Activities.

      1) DNS Technical Assistance activities are for targeting specific S&S topical areas where a Field Office lacks depth or certain capabilities that are otherwise unavailable. Examples of specific areas that may require technical assistance include reviews of Closed Area (Vault-Type Rooms) operations, Material Control and Accountability (MC&A) Programs, Physical Security Systems, and Protective Force EMETL implementation.

      2) Technical assistance activities may also include focused reviews of a specific topical/functional area using an implementation panel or peer review, and may employ SMEs from across the NSE. DNS will partner with the Field Offices to identify topical areas that can benefit from this approach.

      3) DNS may provide SMEs from its Field Augmentation Cadre (FAC), DNS staff, or other Field Offices to support activities at the field-level. This support activity does not relieve a Field Office of its line oversight responsibilities, but can fill a supporting role, as needed.

      4) DNS is responsible for providing oversight of FAC resources, along with coordination, scheduling of support, and vetting all Field Office requests for assistance. The FAC SMEs must be adequately trained to support Field Office self-assessments, surveys, or other initiatives. Field Offices needing any type of support should complete a Request for Program Office Support form to document their needs (refer to Appendix 5, Request for Program Office Support Form). Once the request is approved by the Director, Office of Security Operations and Programmatic Planning, arrangements will be completed with the respective AMSS.

b. Site Assistance Visits (SAV).

1) DNS may conduct a site assistance visit with Field Offices and contractors. The goal is to provide assistance through collaboration in identifying and addressing insufficient protective measures, planning needs, and providing solutions to increase security protection for resources. The need for a site assistance visit could be determined by, but are not limited to, the following factors:

a) A request from the Field Office (e.g., Field Office Manager or AMSS);

b) Data retrieved from operational awareness sources indicating potential problem areas;

c) Results of past inspection reports and/or Field Office surveys to include findings or major challenges at the site and across the NSE;

d) NSE-wide high interest areas or special emphasis items; and,

e) Prior to an EA inspection and based on a support request from the Field Office–ideally the SAV should be performed at least six months in advance of an EA inspection in-brief.

2) Pre-planning meetings convened by the assigned site assistance visit team lead will provide information regarding the scope of the visit and establish expectations for team members. This information could be relayed by several means such as face-to-face, teleconference, or video teleconference. A security review plan (refer to Appendix 6, DNS Security Review Plan Content) will be provided to the Field Office at least 30 calendar days prior to the activity. During the team planning phase, Site Assistance Visit team members are expected to:

a) Become familiar with the results of previous operational awareness and performance assessment activities conducted by EA or other assessment organizations;

b) Review site findings, corrective action plans, IOSCs, deviations status, etc.;

c) Review the objectives and scope of the activity, and any leadership guidance and expectations;

d) Determine appropriate data collection methods and plans, including any necessary performance test plans;

e) Develop a schedule of on-site data collection and related activities;

f) Develop lines of inquiry for topical areas to be reviewed; and,

g) Identify additional information and logistical requirements.

3) The site assistance visit team lead will be a DNS Federal staff member. The team lead will conduct an in-briefing with the Field Office Manager and the AMSS. Site assistance visit team members will attend the in-briefing, and the following information will be provided:

a) Introduction of team members;

b) Objectives and basic scope of the site assistance visit;

c) Coordination of interviews;

d) Discussion of daily team lead updates for the Field Office Manager and AMSS; and,

e) Confirmation of out-briefing time and date.

4) The on-site phase of the site assistance visit is that portion devoted to collecting and validating information obtained through interviews, document reviews, observations of operations, and performance testing. This phase will involve a critical review of all information to provide supportable conclusions. At the site assistance visit team lead's discretion all team members will discuss their activities at end-of-day meetings. Additionally, team members will finalize a synopsis of their activities to be provided to the team lead for developing the out-briefing. Data collection and analysis results will be included in the site assistance visit out-briefing and final report.

5) The out-briefing will be provided to the Field Office Manager and AMSS, to include a list of issues and recommendations that were identified during the site assistance visit. A final report will be developed (refer to Appendix 7, DNS Security Review Report Content), within 21 calendar days after the conclusion of the site assistance visit. Copies will be provided to the Field Office and the CDNS.

c. Special Emphasis Reviews.

1) A DNS Special Emphasis Review (also known as a "For Cause" Review) is driven principally by DNS interests or concerns and emergent issues identified in specific topical areas or at the request of the Field Office Manager or AMSS. The need for a special emphasis review is based on, but not limited to the following items:

a) Recurrence of problems at individual sites or across the NSE;

b) Past performance (negative issues and trends) during EA inspections, Office of Inspector General, and/or Government Accountability Office reviews/assessments;

c) Security incidents; and,

d) Significant issues or degradation in performance.

2) A DNS Federal staff member will lead the review team and may be supported by the FAC or other field SMEs. Several factors are considered during the review:

a) Determine whether the implementation, management, execution, and/or oversight of targeted/specific S&S Program components comply with established policy requirements, and evaluate whether those components are achieving required effectiveness;

b) Evaluate the impact of identified deficiencies, taking into account mitigating factors, compensatory measures, and current or planned corrective actions; and,

c) Identify opportunities for enhancements to strengthen the implementation of S&S programs.

3) Reports developed during special emphasis reviews must clearly document issues discovered, to include potential risks, and should offer expert-level recommendations to mitigate such issues. DNS will complete a final report no later than 21 calendar days following completion of the on-site review (refer to Appendix 7, DNS Security Review Report Content). NA-71 SMEs are given ten calendar days to review and provide comment/feedback on the final report. The final report is issued under the signature of the CDNS and distributed, as appropriate. Any findings identified are recorded in the SSIMS database by the Field Office, and DNS will monitor until closure.

d. Programmatic Reviews.

1) Programmatic reviews represent another key process for gathering information and will be balanced with other performance activities. This will assist in ensuring that the contractor is meeting S&S requirements in protecting NNSA assets and interests.

2) DNS will conduct programmatic reviews across the NSE to determine the level of security program implementation in accordance with requirements. This will also help DNS understand where additional guidance, direction, and resources are needed for security standardization. Programmatic reviews will provide the CDNS confidence that resources

are properly allocated and assist with capturing value-added performance assurance information for NNSA management.

3) Programmatic reviews can be broad or focused on a specific topic of interest, such as locks and keys or entry control procedures, but are not intended to address matter of serious concern for which a "DNS Special Emphasis Review" would be more appropriate. These programmatic reviews are designed to ensure a clear understanding of the S&S oversight programs and functions. The process is used to complement operational awareness and other security activities in collaboration with Field Offices. It is also intended to obtain validation for quarterly deliverables, such as the site security AOP, Protective Force Supplemental and Physical Security Systems Supplemental, and construction projects to assist in determining the effectiveness of performance in implementing S&S programs.

4) DNS will use site integrated assessment plans to include past performance and leadership priorities in coordination with Field Offices to conduct programmatic reviews. DNS will identify and coordinate the selected activity with the applicable Field Office Managers and/or AMSS.

5) DNS representatives during a programmatic review will observe and address program implementation of S&S activities. DNS representatives will provide daily feedback of the activity with recommendations and/or opportunities for improvement to the CDNS, Field Office Manager, and/or AMSS. A written summary report is provided within seven calendar days from completion of the review.

e. Enterprise Assessments Protocols.

1) Protocols are executed in support of EA to enhance the effectiveness of the assessment process. The goal is to ensure that DNS receives timely and appropriate feedback regarding EA results. This information is beneficial in assisting DNS and Field Offices' understanding of the independent assessment of S&S program effectiveness at NNSA sites.

2) NA-71 will typically assign a program manager, desk officer, and/or other DNS security experts, as necessary to each assessment based on their technical qualifications and knowledge of areas to be assessed. SMEs may be assigned to specific aspects of the EA assessment to include force-on-force planning, materials measurement verification, vulnerability assessments, etc. The representatives will serve as support for Field Offices during the scoping, planning, execution, and issue/finding formulation processes of assessments. The NA-71 SME will capture crosscutting policies, performance issues, and best practices that could impact the entire NSE.

3) The DNS representative will actively support the Field Office’s S&S staff during the assessment process to include on-site coordination support that will encompass, but not be limited to the following objectives:

a) Identify emerging issues that are of interest to DNS;

b) Assist with identifying potential issues that surface during initial coordination and execution of the assessment;

c) Provide daily reports to the CDNS and NA-71 staff;

d) Attend the formal EA out-briefing of assessment results;

e) Coordinate with program managers, as appropriate, consistent with issues identified in assessment reports;

f) Work with the Field Office’s S&S staff in providing timely communications to DNS leadership regarding final results of the assessment;

g) Conduct a review of the draft report concurrently with the Field Office S&S staff;

h) Assist the Field Office’s S&S staff, as requested, with the review of corrective action(s) in determining the adequacy of the corrective action (commensurate with the risk associated with the findings); and,

i) Assist in determining if the corrective action(s) are within the Field Office’s purview to resolve or if Headquarters is required to address the issue.

4) The Field Office will ensure that DNS is provided a draft copy of the EA assessment report upon initial delivery and a review of the document should be conducted concurrently between organizations. The Field Office is responsible for the consolidation of EA assessment report comments from all parties to include DNS and contractors for a single response. DNS and Field Office will then evaluate comments prior to DNS submitting the information to EA.

5) DNS will receive the draft comments resolution matrix from EA and disseminate information back to NA-71 SMEs and Field Office AMSS for any additional input. DNS is responsible for feedback consolidation from NA-71 SMEs and Field Office of the EA resolution matrix.

6) DNS representatives and Field Office AMSS will conduct a face-to-face or video teleconference discussion with the EA team after receiving NA-71 SMEs and Field Office feedback on the EA comment resolution matrix.

A minimum of seven calendar days is required for an internal review by NA-71 SMEs and Field Office prior to establishing this meeting with EA. All Federal DNS representatives and the desk officer present during the EA assessment should participate in the discussion to ensure issues are identified and addressed prior to dissemination of the final EA assessment report.

7) Disagreements regarding EA assessments are to be resolved at the lowest possible organizational level. However, if unable to resolve major issues or findings, elevate to the CDNS to achieve resolution.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX 3: DNS AND FIELD OFFICE COMMUNICATIONS

1. Effective communications between DNS and Field Offices provides a feedback mechanism (video teleconferencing, recurring meetings, etc.) to strengthen S&S programs, processes, and procedures. The NNSA S&S Program requires a strong partnership and transparency between DNS and the field, built on trust and open dialog.

2. Field Offices must communicate with DNS regarding their activities and challenges. DNS must provide prompt responses or status updates to Field Offices. The following are several mechanisms as a means to facilitate and increase communications:

   a. Daily Interaction.

   DNS and Field Offices will have daily interaction on several levels regarding the S&S mission and functions. This information could involve the CDNS, Field Office Manager, AMSS, or S&S staffs. An effective exchange of information is crucial to the success of NSE operations.

   b. Conference Calls.

   Conference calls communicate up-to-date status information of S&S Program implementation, and provide a forum to discuss current and emerging issues raised by Headquarters leadership or the field. NA-71 hosts a bi-weekly conference call with all of the AMSSs (or equivalent), and the CDNS conducts a monthly call with individual Field Office AMSSs to discuss site-specific S&S issues.

   c. Quarterly and Periodic Meetings.

   DNS conducts quarterly and supplemental periodic meetings with the field leadership, as needed. These forums include S&S meetings and budget execution reviews. In addition to the normal course of business at these meetings, DNS may provide an opportunity to discuss expectations, budgetary issues, achievements, and challenges; best practices; evaluate S&S programs from various perspectives; and provide feedback and open dialog between Headquarters and the field.

   d. NNSA Event Notification Matrix.

   The NNSA Event Notification Matrix is used by site personnel to alert senior leadership of incidents or events at NNSA locations, within a designated timeline (refer to Appendix 8, NNSA Event Notification Matrix).

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX 4: FIELD SECURITY SURVEY AND SELF-ASSESSMENT REPORT CONTENT

FIELD SECURITY SURVEY AND SELF-ASSESSMENT REPORT CONTENT	
Executive Summary	• The scope, methodology, period of coverage, duration, and date of the exit briefing to Field Office management • Brief overview of the facility, function, scope of operations, and contractual information • Brief synopsis of major strengths and weaknesses that impact the effectiveness of the facility's overall S&S program, including identification of topical areas rated less than satisfactory • Overall composite facility rating (e.g., Marginal, Satisfactory, Unsatisfactory) with supporting rationale • Reference to a list of findings identified during the survey or self-assessment
Introduction	• Scope, methodology, period of coverage, duration, and date of the exit briefing to Field Office management • Description of the facility, its function and scope of operations, security interests, and contractual information
Narrative	• Description of the site's implementation of the S&S program function • Scope of the evaluation • Description of activities conducted • Evaluation results and associated issues (including other Department organizations or Other Government Agencies review or inspection results related to this topical and sub-topical that were included in the survey) • Identification of all findings, including new and previously identified open findings, regardless of source (e.g., EA, IG, GAO), and their current corrective action status • Analysis provides justification and rationale of factors responsible for the rating
Attachment (s) *As Applicable*	• Completed DOE F 470.8, Department of Energy Survey/Inspection Report Form • Completed DOE F 470.2, Facility Data and Approval Record (FDAR) • Active DOE F 470.1, Contract Security Classification Specification (CSCS), or DD F 254, Contract Security Classification Specification • New findings resulting from the survey/self-assessment • Previous findings that are open, to include the current status of corrective action • Team members including names, and their assigned area(s) of evaluation • Source documentation used to support the survey/self-assessment (e.g., EA, IG, GAO, and similar assessment documents)

To Be Completed by the Field Office

Signature:____ _______________
Team Leader Date

Concurrence:____________________________________ _______________
Assistant Manager for Safeguards and Security Date

Approval:____ _______________
Field Office Manager Date

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX 5: REQUEST FOR PROGRAM OFFICE SUPPORT FORM

REQUEST FOR PROGRAM OFFICE SUPPORT			
Field Office Requesting Support			
□Kansas City	□Livermore	□Los Alamos	□Nevada
□NPO - Pantex	□NPO - Y-12	□Sandia	□Savannah River
Field Office Point of Contact: *Name/Phone Number*		Date(s) Support is Needed: *Month/Day/Year* To *Month/Day/Year*	
Date Request Submitted: *Month/Day/Year*			
Type of Support Requested: □Survey Augmentation □Other Programmatic Support			
Justification for Request: *Provide Justification/Reasons for Request*			
Detailed Scope of Work: *Provide Detailed Description of Work and Level of Effort*			
To Be Completed by NA-70			
Estimated Cost ($K):		Scheduled Date:	

Signature:________________________________ ______________
Team Leader Date

Approval:______________________________ ______________
Director, NA-71 Date

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX 6: DNS SECURITY REVIEW PLAN CONTENT

DNS SECURITY REVIEW PLAN CONTENT	
Field Office	(State Field Office to be reviewed)
Review Date and Schedule	(Give dates of review activities and a schedule that will be followed)
Scope	(State Scope of DNS review)
Methodology	(Provide a brief description of the methodology that will be used in the DNS review)
Activities to be Observed	(Identify the specific S&S topical areas/sub-topical areas to be reviewed)
DNS Review Team Evaluator	(Identify DNS team leader and team members)
Documents to be Reviewed	(List documents to be reviewed as part of the review to include: • Field Office survey or self-assessment report • Field oversight process/procedure documentation • Field Office performance assurance program documentation • Most recent Office of Enterprise Assessments report of the site • Most recent Field Office survey or self-assessment • Documents outlining roles and responsibilities)
Field Office POC	(State Field Office Point of Contact)
Site Support Needed	(List site personnel required and that will be interviewed)
References	(List references that will be used)

DNS Review Plan Prepared by:___________________________________ Date____________

Approval:______________________________ _______________
Director, NA-71 Date

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX 7: DNS SECURITY REVIEW REPORT CONTENT

DNS SECURITY REVIEW REPORT CONTENT	
Review Type	(State the type of activity to be reviewed)
Field Office	(State Field Office to be reviewed)
Field Office POC	(State Field Office Point of Contact)
Executive Summary	(List summary information concerning the review to include a brief description of the facility, and a synopsis of major weaknesses that impact effectiveness of the activity being reviewed)
Objective	(A brief statement on the objective of the review)
Scope	(State scope of DNS Review and what the review was to address)
References	(Provide a list of references)
DNS Review Team Evaluator	(Identify DNS team lead and team members)
Field Office Team Members	(List the Review team members and their responsibilities)
Activities Observed	(Identify the specific S&S topical areas/sub-topical areas that were reviewed)
Documents Reviewed	(List documents that were reviewed)
Personnel Interviewed	(Identify the personnel interviewed)
Findings/Observations	(Findings/Observations should include enough detail to clearly understand the issue. The narrative section of the report should describe the facility's S&S interests and activities, its protective measures, and the status of the S&S activity at the time of the review. The report should also explain how the protection measures were evaluated)
Point of Contact	(Provide the team leader and phone number/e-mail to address questions on the report)

Signature:________________________________ ______________
Team Leader Date

Concurrence:_____________________________ ______________
Director, NA-71 Date

Approval:_________________________________ ______________
Chief, Defense Nuclear Security Date

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX 8: NNSA EVENT NOTIFICATION MATRIX

INITIATING EVENT	IM	NEXT BUSINESS DAY/ NIGHT NOTE	HQ EOC	AMSS	FOM	NA-IM	CDNS	NA-3	NA-2	NA-1
Active shooter incident	x		x	x	x		x	x	x	x
Aircraft encounter/incursion that raises security interest	x		x	x	x		x	x	*	*
Arson	x		x	x	x		x	x	x	x
Off-site arrest (Protective Force and/or Human Reliability Program [HRP] certified)		x		x	x		x			
Assault w/injury require hospitalization occurring on or off-duty	x			x	x		x	x	x	x
Animal incidents (i.e., dangerous/rabid and/or involving endangered species)		x		x			x			
Bomb threat	x		x	x	x		x		*	*
Boundary/Fence Line Break (Cuts/Breaks/Holes) Property Protection Area (PPA)/General Access Area (suspected or confirmed intrusion, or apparent attempted intrusion)	x		x	x	x		x	x	*	*
Catastrophic communication system failure (over 30 mins) that impacts security	x		x	x	x	x	x			
Compensatory measures: (Those measures lasting more than eight hours)		x		x	x		x			

INITIATING EVENT	IM	NEXT BUSINESS DAY/ NIGHT NOTE	HQ EOC	AMSS	FOM	NA-IM	CDNS	NA-3	NA-2	NA-1
Confirmed inventory difference of Special Nuclear Materials (SNM)	x			x	x		x	x	x	x
Confirmed loss/compromise of classified	x			x	x	x	x	x	x	x
Confirmed missing person on NNSA property	x		x	x	x		x	x	x	x
Counterintelligence event (individual act and/or intelligence service)	x		x	x	x	x	x	x	x	x
Damage to government property (>100k)	x		x	x	x	x	x	x	x	x
Damage to government property (>25K<$100K)		x	x			x	x	x	x	x
Damage to government property (<$25K)		x		x		x	x			
Demonstration (small and peaceful)		x		x	x		x	x		
Demonstration (large or arrest)	x		x	x	x		x	x	*	*
Domestic dispute/violence (Lautenberg Amendment-Protective Force and or HRP certified)	x			x	x		x			
Drug Arrest HRP certified and/or Protective Force (federal/contractor employees)		x		x	x		x			
Facility lockdown as a result of security threat requiring posture	x	x	x	x	x	x	x	x	*	*

INITIATING EVENT	IM	NEXT BUSINESS DAY/ NIGHT NOTE	HQ EOC	AMSS	FOM	NA-IM	CDNS	NA-3	NA-2	NA-1
change or safety/environmental hazard, such as a chemical spill or radiological release										
Fatality (on-site)	x		x	x	x		x	x	x	x
Fire (small – non-critical area/contained)		x		x				x		
Fire (large – critical area/not contained)	x		x	x	x		x	x	x	x
Flood (significant damage or disrupting operations)	x		x	x	x		x	x	x	x
Forced entry (critical area)	x		x	x	x		x	x	*	*
Forced entry (non-critical area)		x		x	x		x			
Gate crasher/runner		x	x	x	x		x	x		
Hazardous materials accident	x		x	x	x		x	x	x	x
Homicide (off-site) involving NNSA personnel		x	x	x	x		x	x	x	x
Hostage situation	x		x	x	x		x	x	x	x
Inclement weather that forces change in security posture	x		x	x	x		x	x		
Intrusion (suspected and or confirmed) Limited Area/Protection Area (PA)	x		x	x	x		x	x	*	*
Labor strike	x		x	x	x		x	x	x	x
Media/Press on-site (announced/ unannounced)	x			x	x		x	x	x	x

INITIATING EVENT	IM	NEXT BUSINESS DAY/ NIGHT NOTE	HQ EOC	AMSS	FOM	NA-IM	CDNS	NA-3	NA-2	NA-1
Medical emergency that requires 911 response		x	x	x	x		x			
Off-site arrest (Protective Force and/or HRP certified)		x		x	x		x			
On-site drug arrest (federal/contractor employees)		x		x	x		x			
On-site vehicle accident (w/injury)	x		x	x	x		x			
On-site weapons discharge	x			x	x		x	x	*	*
Personally Identifiable Information is compromised (or compromise cannot be ruled out)	x			x	x	x	x	x	x	x
Physical security system failure negatively impacting protection strategy effectiveness	x		x	x	x	x	x	x	*	*
Power outage (impacting security)		x	x	x		x	x			
Protective Force use of force violation	x			x	x		x	x	*	*
Robbery		x	x	x	x	x	x	x	x	x
Sabotage (including potential acts)	x		x	x	x		x	x	x	x
Security Police Officer (SPO) misconduct that requires formal corrective action		x		x	x		x			
Serious injury (on-site)	x		x	x	x		x	x	*	*
Serious injury (off-site)		x	x		x		x	x	*	*
Site, laboratory, or plant closure	x		x	x	x		x	x	x	x

INITIATING EVENT	IM	NEXT BUSINESS DAY/ NIGHT NOTE	HQ EOC	AMSS	FOM	NA-IM	CDNS	NA-3	NA-2	NA-1
Special Access Programs (SAP) incident	x		x	x	x	x	x	x	x	x
Suicide (confirmed)	x		x	x	x		x	x	x	x
Suicide (attempt)	x		x	x	x		x	x	*	*
Suspected/confirmed physical surveillance of NNSA facility	x		x	x	x		x			
Theft >$500 or displays a pattern		x	x	x	x	x	x	x	*	*
Threat of physical violence towards off-duty employee based on their association with the US government	x		x	x	x		x	x		
Threat to departmental assets	x		x	x	x		x	x	x	x
Trespassing of PPA	x			x	x		x	x	*	*
Technical Surveillance Countermeasures incident	x			x	x	x	x	x	x	x
Unexplained process difference of SMN that causes security concern		x	x	x	x		x	x	x	x
Unexplained shipper receiver difference of SNM	x			x	x		x	x	x	x
Unlawful Protective Force detention (including potential)		x	x	x	x		x	x	*	*
Unauthorized entry attempt of Limited Area and/or PA	x		x	x	x		x	x	*	*
Unauthorized movement of nuclear material	x		x	x	x		x	x	*	*
Unauthorized unmanned aerial systems	x		x	x	x		x	x	*	*

INITIATING EVENT	IM	NEXT BUSINESS DAY/ NIGHT NOTE	HQ EOC	AMSS	FOM	NA-IM	CDNS	NA-3	NA-2	NA-1
(UAS)/unmanned aerial vehicles (UAV)										
Unsecured building containing classified matter		x		x			x			
Waste, fraud, and abuse (security related)		x		x	x	x	x	x		
Workplace violence incident		x	x	x	x		x	x	x	x
CYBER SECURITY EVENTS										
Attempted or unauthorized access of a computer system		x		x	x	x	x	x		
Classified spillage	x		x	x	x	x	x	x	*	*
Critical infrastructure protection impacted by an adverse cyber event/action	x		x	x	x	x	x	x	x	x
Denial of service attack	x		x	x	x	x	x	x	x	x
Loss, theft, missing IT resources		x		x	x	x	x	*	*	*
Malicious code infection that affects computer systems and/or networks	x		x	x	x	x	x	x	x	x
Persistent surveillance and resource mapping probes and scans that stand out above daily noise level	x		x	x	x	x	x	x	x	x
System compromise/intrusion	x		x	x	x	x	x	x	x	x
Unauthorized usage of a government computer system		x		x	x	x	x	*	*	*

**Notifications TBD by CDNS/NA-3 and higher*

CATEGORY	**METHOD**
IMNOT Immediate notification, not to exceed (1) hour from time of discovery	**Landline**
Notification to occur either the next business day or through a Night Note	**Landline or Electronic Means**

INCIDENT REPORTING GUIDELINES

INTENT: The following event notification guidelines are a set of business rules intended to provide a clear process for notifying key DOE/NNSA personnel in a timely manner of incidents involving the security of nuclear weapons, special nuclear material, or incidents affecting NNSA personnel, facilities, or property. Recent events where established protocols were followed revealed a disconnect between the established notification processes and actual expectations. This notification matrix will eventually be incorporated in DOE policy.

NOTIFICATION TIMELINES: The notification timelines provide an expectation for notifying key DOE/NNSA personnel in a timely manner, depending on the dynamics of the event. There is no expectation for this notification process to take precedence over the immediate handling of the incident by the local leadership team. In all instances, addressing the incident is always the primary concern of local management, when the situation permits the following timelines will be followed:

A. ***Immediate Notification (IMNOT)* –** Notify key headquarters DOE/NNSA personnel immediately of an event that falls into this notification category. Time lapse from discovery of the incident to notification to CDNS should not exceed (1) hour. Notification requirements must provide minimal details (who, what, when, where, and how) to ensure key personnel have situational awareness of the event and are able to brief external stakeholders and leadership as required. Immediate notifications require telephonic contact with key personnel or designee at the contact numbers provided. Follow-up notifications should be made as details become available or as requested.

B. ***Next Business Day or Night Note* –** Incidents in this category should be briefed to key headquarter NNSA personnel or designee via telephonic contact or written correspondence (email), via a night note or the next business day. The correspondence should provide all known details (who, what, when, where, and how) and current status of the incident.

RESPONSIBILITY: Notification to key headquarters DOE/NNSA personnel or designee of any reportable event is the responsibility of the Field Office Manager and staff as directed locally. The key personnel or designee receiving the notification will convey the information to the next level of leadership as required.

NOTIFICATION MATRIX: The notification matrix is a situational document, which provides incidents and events for which key DOE/NNSA personnel, external stakeholders, and leadership requires notification from the responsible field element, within the designated timeline. The field elements should use a conservative decision-making approach for any incident or event not contained in the notification matrix.

NNSA EVENT NOTIFICATION CHECKLIST: NNSA event notification checklist provides guidance of required information sets that must be included in the notification to DOE/NNSA personnel or designee.

NNSA EVENT NOTIFICATION CHECKLIST

This notification checklist is designed to aid/guide in making initial notification to the Office of Defense Nuclear Security and key DOE/NNSA personnel. Please provide the completed information listed below and any other pertinent information when making initial notification to the DOE/NNSA Headquarters personnel. If this document is used, it must be reviewed by a derivative classifier before transmitting via unclassified means.

1. **Site location, Discovery Date, and Time Incident was reported to HQ.**

2. **Description of Incident –** Information relevant to the incident (who, what, where, when, how, and Category of Incident).

3. **Describe the initial steps taken to mitigate the incident.**

4. **Timeline of Incident –** Record date and time of the incident (include time of discovery, response, and sequence of events).

5. **Is a formal Damage Assessment warranted?**

6. **Involve Foreign Nationals?**

7. **Media Exposure?**

8. **Was there any injury or medical response?**

9. **Point-of-Contact and Information –** Provide a Point-of-Contact and contact information for immediate clarification and update.