SUPPLEMENTAL DIRECTIVE

NNSA SD 226.1-2

Approved: 05-25-21
Expires: 05-25-24

DEFENSE NUCLEAR SECURITY GOVERNANCE

NATIONAL NUCLEAR SECURITY ADMINISTRATION
Office of Defense Nuclear Security

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

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

DEFENSE NUCLEAR SECURITY GOVERNANCE

1. PURPOSE. To establish a foundation for effective, efficient, and integrated safeguards and security (S&S) oversight. Under the National Nuclear Security Administration (NNSA) governance structure, the Office of Defense Nuclear Security (DNS) serves as both a program and functional office, and shares responsibility with field offices for functional performance. This Supplemental Directive (SD) clarifies roles and responsibilities for program, functional, and field office portions of S&S oversight in pursuit of accomplishing and sustaining mission work at the NNSA labs, plants, and sites, collectively known as the nuclear security enterprise (NSE).

2. AUTHORITY. This SD supplements the requirements of Department of Energy (DOE) Policy 226.2, *Department of Energy Oversight Policy*, DOE Order 226.1B, *Implementation of DOE Oversight Policy*, and NNSA SD 226.1C, *NNSA Site Governance*.

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

4. APPLICABILITY.

   a. Federal. This SD applies to NNSA federal employees within DNS and NNSA field offices. This SD automatically applies to NNSA elements within DNS and field offices that are created after the SD is issued.

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

   c. Equivalencies/Exemptions.

      (1) Equivalency.

         (a) 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/Department of Energy (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.

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

         (c) In accordance with the responsibilities and authorities, and to ensure consistency within the Office of Secure Transportation, the

NNSA Deputy Administrator for Defense Programs will implement and oversee requirements and practices pertaining to this Directive for activities under the Deputy Administrator's cognizance, as deemed appropriate.

(2) Exemptions. None

5. SUMMARY OF CHANGES. This SD replaces NNSA SD 470.4-1, *Defense Nuclear Security Federal Oversight Process,* with requirements and responsibilities, including those for headquarters and field office personnel, for federal S&S oversight at NNSA facilities in accordance with the *NNSA Governance & Management Framework* and NNSA SD 226.1C, *NNSA Site Governance*.

6. BACKGROUND. Four DNS positions constitute the program office and jointly fulfill program office oversight roles:

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

b. Deputy Associate Administrator for DNS

c. Director, DNS Office of Security Operations and Programmatic Planning

d. Director, DNS Office of Personnel and Facility Clearances and Classification.

7. REQUIREMENTS. All S&S programs, practices, and procedures developed within NNSA must be consistent with all DOE and national requirements (e.g., Atomic Energy Act of 1954, Executive Orders, U.S. Code, Code of Federal Regulations). Routine S&S oversight activities are defined at the Program, Functional, and Field levels to achieve consistency with the *NNSA Governance & Management Framework* while also allowing for flexibility in oversight application to account for the unique needs and priorities of individual sites. Where applicable, communications between program, functional, and field offices must follow the process specified in Appendix A.

a. Program Office Oversight. The program office must conduct oversight by carrying out the following activities:

(1) Operational Awareness.

(a) Identify NSE S&S program priorities, issues, and trends using complex-wide operational awareness data that has been collected, filtered, and analyzed by functional and field offices.

(b) Identify the data type and frequency required for maintaining operational awareness over S&S program execution across the NSE, in collaboration with functional and field offices.

(c) Maintain complex-wide operational awareness by leveraging analytical products that functional offices create, which are based on information provided by field oversight activities, according to programmatic guidance and S&S mission objectives.

(2) Contractor Assurance Verification. Program-level contractor assurance verification is enabled by field offices, which collect and verify contractor assurance data, and functional offices, which identify trends within their competencies across sites.

(a) Monitor contract partner performance on scope, cost, and schedule using contractor assurance data and associated field office analysis.

(b) Provide continuous feedback on contractor assurance system activities in coordination with the field office.

(3) Assessments.

(a) Identify the scope and schedule of DNS-led programmatic assessments where warranted, either by statute or on the basis of mission risk.[1]

(b) Coordinate with functional offices and field management to schedule assessment activities using the Site Integrated Assessment Plan (SIAP) drafting and review process.

(c) Establish a process, in conjunction with functional and field offices, by which to assess the implementation of delegated Officially Designated Federal Security Authority (ODFSA) and NNSA Chief Security Officer (CSO) authorities. This process and the results are shared with all functional and field offices.

(4) Planning.

(a) Establish S&S performance objectives and other evaluation criteria for contractors that evaluate contractor performance, in coordination with functional and field offices, for use in the Corporate Performance Evaluation Process.

(b) Evaluate site- and NSE-wide S&S topics identified by functional offices each fiscal year as candidates for focused assessment during the upcoming fiscal year and develop site- and enterprise-wide recommendations on these topics.

[1] This SD does not govern DNS participation in assessments directed by external entities (e.g., U.S. Department of Energy Office of Enterprise Assessments).

(c) Coordinate and transmit program-level recommendations for focused assessment activities to field offices for incorporation into the SIAP development process.

(d) Review finalized SIAPs and field assessment lists prioritized by the functional offices. Develop field assessment participation schedules for each functional office.

(e) Provide schedules for functional office participation in field assessments to field offices.

(5) Documentation and Communication of Oversight Activities.

(a) Document oversight activities in accordance with standard operating procedures.

(b) Communicate programmatic priorities, trends, and issues to functional and field office management and other relevant program offices within the NSE.

(c) Follow established protocols to communicate with contractors regarding oversight expectations and performance and include relevant program, functional, and field office stakeholders.

b. Functional Office Oversight. The functional office comprises federal personnel assigned by the program office to support the implementation of federal S&S oversight. The functional office serves as the conduit between the field offices and the program office supporting the latter by evaluating S&S program execution in conjunction with field offices and identifying enterprise-level trends within each S&S functional area using data provided by field offices. The DNS functional office includes functional area managers and site operations officers.

Functional office personnel perform defined regulatory functions and oversight support in consultation with the program office and field offices. Oversight support is provided in accordance with guidance, strategy, and priorities set by the program office and is carried out in concert with the field office to collect and analyze the data necessary to meet program office expectations. Activities performed by functional office personnel working in the field to augment field S&S oversight capabilities are considered to be field oversight activities.

Functional office oversight must be implemented through the following activities:

(1) Operational Awareness.

(a) Maintain complex-wide operational awareness within each functional area by leveraging information provided by field oversight activities in accordance with programmatic guidance and S&S mission objectives.

(b) Identify NSE-wide S&S program priorities, issues, and trends within each functional area and report the results to relevant program offices to be evaluated for applicability in future field oversight activities.

(2) Contractor Assurance Verification. Primarily a field office activity; however, functional offices may need to collaborate with field offices to review collected contractor assurance data that supports a functional review of enterprise-wide trends, based on priorities established by the program office.

(3) Assessments. Support program-level assessments (i.e., those related to delegated ODFSA responsibilities) based on scope and schedule where warranted, either by statute or on the basis of mission risk associated with a security event or emerging security concern. Program-level assessments focus on evaluating the effectiveness of field office oversight of contractor performance in delegated areas.

(4) Planning.

(a) Use operational awareness data and lessons learned to identify site- and NSE-wide S&S topics prior to the end of the third quarter of each fiscal year, for potential focused assessment during the upcoming fiscal year. Identified focus areas are provided to the program office to be evaluated for transmission to the field office.

(b) Review finalized SIAPs. Provide the program office with a prioritized list of focused field office assessments in which the functional office has been requested to support or participate, or in which the functional office would like to participate.

(5) Documentation and Communication of Oversight Activities.

(a) Document oversight activities in accordance with standard operating procedures.

(b) Communicate with field offices, including all stakeholders, regarding oversight expectations and desired performance in accordance with established protocols.

(c) Communicate the purpose and results (including trends and issues) from functional office analyses of operational awareness data (e.g., incidents of security concern monthly reports) to relevant program and field offices.

(d) Include relevant field office personnel in all communications between functional offices and contractors.

c. Field Office Oversight. Field offices are part of federal line management and perform oversight activities to evaluate contractor performance and manage risk-enabling contractors to execute NNSA mission work effectively, efficiently, and within the bounds of regulatory compliance.

In conducting their oversight activities, field offices maintain day-to-day operational awareness of contractor activities leveraging contractor assurance system data and implementing formal assessments. Field offices communicate performance information to field management, functional, and program offices to support enterprise-level programs and risk decisions. Field office oversight implementation is tailored to the level of risk associated with each functional office relevant to the facility or site.

The field office must conduct oversight by carrying out the following activities.

(1) Operational Awareness Activities (OAAs).

(a) Conduct OAAs and provide local site management an understanding of day-to-day contractor performance of ongoing operations at the site.

i. OAAs can include activities such as attending contractor meetings, reviewing data and metrics, reviewing management reports, and observing contractor work activities.

ii. OAAs can be planned or conducted ad hoc to meet field, functional, or program-level objectives.

(b) Evaluate OAA data to determine local trends that may need further evaluation.

(c) Provide functional offices with data used by the functional office to maintain operational awareness.

(2) Contractor Assurance Verification.

(a) Review contractor assurance system S&S performance and data communication.

(b) Evaluate the effectiveness of contractor assurance systems using program identified NSE-wide S&S program priorities, issues, and trends.

(c) Apply results from local contractor assurance system analyses to plan future oversight activities.

(d) Communicate local site trends and insights from contractor assurance activities to field management and the program office. This information will be shared with appropriate functional offices for evaluation of complex-wide issues or trends.

(e) Determine timelines for closure of federally identified issues that are commensurate with the mission risk posed by the issue.

(3) Assessments. Field offices participate in internal and external assessments to determine contractor performance in the implementation of a specific functional area, sub-area, or activity at a particular point in time. Types of assessments include security surveys, shadow assessments, and self-assessments. Assessments are planned in advance and are listed in each field office's SIAP.

(a) Coordinate and consolidate assessments to meet identified functional and program office needs.

(b) Identify schedules and resource needs during the assessment planning process.

(c) Conduct program-level assessments with support from functional subject matter experts as necessary.

(4) Planning.

(a) Utilize field procedures to conduct a risk-based review of oversight areas for use in SIAP development. Include function or site-specific emphasis areas from any known vulnerabilities or performance weaknesses that pose a high risk to mission execution for the upcoming year.

(b) Consider program office recommendations for focused assessments when developing the SIAP.

(c) Include field requests for functional office assistance in the SIAP.

(d) Approve the annual SIAP and submit it in accordance with NNSA SD 226.1C, *NNSA Site Governance*.

(e) Coordinate functional participation of assessment activities identified on the program office participation list.

(f) Request the support of functional offices using established processes, such as the Center for Security Technology, Analysis, Response, and Testing portal, when needed.

(5) Documentation and Communication of Oversight Activities.

(a) Maintain records of OAAs. Documentation of activities will be conducted through locally established processes.

(b) Communicate local priorities, trends, and issues to functional offices for those areas identified by the program office as areas of potential concern, areas related to programmatic initiatives, and areas that may impact the NSE.

(c) Communicate with contractors through established channels.

(d) Provide periodic oversight documentation to contractors through locally established procedures.

8. RESPONSIBILITIES.

a. Chief of Defense Nuclear Security/Associate Administrator for Defense Nuclear Security.

(1) Serves as the NNSA ODFSA and CSO responsible for the development and implementation of S&S programs and operations for NNSA security organizations.

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

(3) Develops implementing guidance and standards related to the NNSA S&S Program.

(4) Develops and allocates the security budget to support the DNS mission.

(5) Establishes strategic vision and multi-year objectives for the nuclear security program.

(6) Provides subject matter experts to support field requests for assistance in functional areas.

b. Field Office Manager/Officially Designated Federal Security Authority.

(1) Implements ODFSA responsibility, as delegated, for security program plans and activities at their specific sites.

(2) Identifies federal roles, responsibilities, and authorities necessary to direct, guide, and oversee security operations at their respective site.

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

(4) Coordinates with Contracting Officers or Contracting Officer Representatives for contractor implementation of S&S programs.

(5) Conducts OAAs.

c. Program Offices.

(1) Develop programmatic guidance and strategy and set mission priorities.

(2) Verify the effective execution of delegated authorities, including *inter alia* ODFSA and NNSA CSO authorities.

(3) Develop oversight guidance, strategy, and priorities on the basis of data collected and analyzed by the functional and field offices.

9. ACRONYMS. See Appendix B

10. DEFINITIONS. See Appendix C

11. REFERENCES.

1. DOE Policy 226.2, *Policy for Federal Oversight and Contractor Assurance Systems*, dated 8-9-16.

2. DOE Order 226.1B, *Implementation of Department of Energy Oversight Policy*, dated 4-25-11.

3. DOE Guide 226.1-2A, *Federal Line Management Oversight of Department of Energy Nuclear Facilities*, dated 4-14-14.

4. DOE Order 470.4B, *Safeguards and Security Program*, dated 1-17-17.

5. DOE Order 473.3A, *Protection Program Operations*, dated 3-23-16.

6. NNSA Supplemental Directive 226.1C, *NNSA Site Governance*, dated 10-1-19.

7. *NNSA Governance & Management Framework*, dated March 2019.

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

BY ORDER OF THE ADMINISTRATOR:

Charles P. Verdon
Acting Administrator

Appendices:
A: NNSA Incident Reporting Guidelines and Event Notification Matrix
B: Acronyms
C: Definitions

APPENDIX A: NATIONAL NUCLEAR SECURITY ADMINISTRATION INCIDENT REPORTING GUIDELINES AND EVENT NOTIFICATION MATRIX

1. INTRODUCTION. The following event notification guidelines are a set of business rules intended to provide a clear process for notifying key Department of Energy/National Nuclear Security Administration (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 in which established protocols were followed revealed a disconnect between the established notification processes and actual expectations. This notification matrix will eventually be incorporated into DOE policy.

2. PROCESS.

   a. 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:

      (1). Immediate Notifications (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 Chief of Defense Nuclear Security (CDNS) should not exceed one 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.

      (2). Next Business Day or Night Note. Incidents in this category should be briefed to key Headquarters 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.

   b. Notification 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.

c. Notification Matrix. The notification matrix is a situational document that 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.

d. NNSA Event Notification Checklist. The 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 Defense Nuclear Security (DNS) and key DOE/NNSA personnel. Please provide the information listed below and any other pertinent information when making initial notification to DOE/NNSA Headquarters (HQ) 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.

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	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
Access Area (suspected or confirmed intrusion, or apparent attempted intrusion)										
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			
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

INITIATING EVENT	IM	NEXT BUSINESS DAY/ NIGHT NOTE	HQ EOC	AMSS	FOM	NA-IM	CDNS	NA-3	NA-2	NA-1
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 change or	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
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

INITIATING EVENT	IM	NEXT BUSINESS DAY/ NIGHT NOTE	HQ EOC	AMSS	FOM	NA-IM	CDNS	NA-3	NA-2	NA-1
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
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	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
compromised (or compromise cannot be ruled out)										
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
Special Access Programs (SAP) incident	x		x	x	x	x	x	x	x	x
Suicide (confirmed)	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
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 U.S. 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 SNM 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	*	*

INITIATING EVENT	IM	NEXT BUSINESS DAY/ NIGHT NOTE	HQ EOC	AMSS	FOM	NA-IM	CDNS	NA-3	NA-2	NA-1
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 aircraft systems (UAS)/unmanned aerial vehicles (UAV)	x		x	x	x		x	x	*	*
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	x		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
an adverse cyber event/action										
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 one hour from time of discovery	**Landline**
Notification to occur either the next business day or through a Night Note	**Landline or Electronic Means**

APPENDIX B: ACRONYMS/ABBREVIATIONS

a. AMSS Assistant Manager for Safeguards and Security
b. CDNS Chief of Defense Nuclear Security
c. CSO Chief Security Officer
d. DNS Defense Nuclear Security
e. FOM Field Office Manager
f. HQ Headquarters
g. HRP Human Reliability Program
h. IM Information Management
i. IMNOT Immediate Notification
j. NA-1 Under Secretary for Nuclear Security and Administrator
k. NA-2 Principal Deputy Administrator
l. NA-3 Associate Principal Deputy Administrator
m. NA-IM Office of the Associate Administrator for Information Management and Chief Information Officer
n. NSE nuclear security enterprise
o. OAA Operational Awareness Activity
p. ODFSA Officially Designated Federal Security Authority
q. PA Protected Area
r. PPA Property Protection Area
s. S&S safeguards and security
t. SAP Special Access Programs
u. SIAP Site Integrated Assessment Plan
v. SNM Special Nuclear Material
w. SPO Security Police Officer
x. UAS unmanned aircraft systems
y. UAV unmanned aerial vehicles

APPENDIX C: DEFINITIONS

a. Assessment. An oversight activity planned and documented in a Site Integrated Assessment Plan and conducted to determine contractor performance in the implementation of a specific functional area, sub-area, or activity at a point in time.

b. Contractor Assurance Verification. A federal oversight activity undertaken to observe or leverage a contractor's own oversight processes in support of operational awareness.

c. Field Office. An NNSA organization responsible for administering performance-based contracts with NNSA contractors to deliver on objectives set by program offices, authorization or approval of contractor activities in accordance with delegated authorities and DOE/NNSA policy, and serving as the U.S. Government's representative at each laboratory, plant, or site (as applicable).

d. Functional Office. An NNSA headquarters organization that is responsible for enabling mission work by providing expertise, advice, and counsel to program offices, senior management, and field offices in accordance with roles established by DOE/NNSA policy and performing defined regulatory functions and oversight support in consultation and coordination with program and field offices.

e. Governance. The system of management and controls executed in the stewardship of the organization. NNSA implements governance through a collaborative partnership between federal and contractor organizations to accomplish a common mission while still preserving the federal independence needed to function in NNSA's self-regulatory role.

f. Officially Designated Federal Security Authority. ODFSAs are federal employees who possess the appropriate knowledge and responsibilities for each situation to which they are assigned through delegation. Delegation authority for these positions is originated according to direction from the accountable Program Secretarial Officer (or the Secretary or Deputy Secretary for Departmental Elements not organized under a Program Secretarial Office), who also provides direction for which of the ODFSA positions may be further delegated. Each delegation must be documented in written form.

g. Operational Awareness. Awareness maintained by federal oversight personnel of program scope, relationships, site resources and capabilities necessary to support program activities and associated risks (e.g., safeguards and security; environment, safety, and health; emergency management; and nuclear operations).

h. Program Office. An NNSA headquarters organization that is responsible for overseeing appropriated funding and executing program management functions. Programs are national in scope and span multiple NNSA sites.

i. Site Integrated Assessment Plan. A document developed for each NNSA laboratory, plant, or site, in accordance with NNSA SD 226.1C, that identifies a comprehensive transparent plan for federal assessment activities for a given fiscal year.

j. Shadow assessment. A shadow assessment is an assessment in which the field offices observe, but do not participate directly in, a contractor's own oversight activities with the dual purpose of gathering information about the area being assessed and for contractor assurance verification.