Chapter 11 Revision History

Subsection	Date	Changed	To
This entire chapter has undergone a major revision. As these changes are too extensive to itemize, *please review Chapter 11 in its entirety.*	01/05/2018		
Sections on Identifying and Categorizing Incidents and Tracking and Trending has been added. A fillable "Notification" template is attached.	11/22/2019		

Chapter 11
Incidents of Security Concern

This chapter covers the DOE HQ implementation of DOE Order 470.4B, Chg. 2, *Safeguards and Security Program, Attachment 5, Incidents of Security Concern.* The Office of Headquarters Security Operations (AU-40) in the Office of Environment, Health, Safety and Security manages the HQ Security Incidents Program.

Incidents of Security Concern (henceforth referred to as Incidents) are actions, inactions, or events that are believed to:

- Pose threats to national security interests and/or DOE assets or degrade the overall effectiveness of DOE's protection program.
- Create potentially serious or dangerous security situations.
- Significantly affect the safeguards and security program's capability to protect DOE safeguards and security interests.
- Indicate failure to adhere to security procedures.
- Reveal the system is not functioning properly, by identifying and/or mitigating potential threats (e.g., detecting suspicious activity, hostile acts, etc.).

Incidents require follow up to:

- Ensure management awareness.
- Determine the facts and circumstances of the incident.
- Ensure corrective actions are taken to mitigate the incident.

- Develop actions to correct underlying weaknesses and prevent recurrence.
- Track and trend incidents to improve the health of the security program.
- Document whether a security infraction or other disciplinary action is needed.

Headquarters Implementation Procedures

Identifying and Categorizing Incidents:

DOE uses a graded approach for identifying and categorizing incidents as described in DOE Order 470.4B, Change 2, *Safeguards and Security Program, Attachment 5 Incidents of Security Concern*. This Order provides greater detail on incident categorization and incident criteria as well as an Incident Categorization Matrix to assist with identification and categorizing of Incidents based on the type of incident event. *DOE Standard Incidents of Security Concern*, DOE-STD-1210-2012, September 2012, also provides information on identifying and categorizing security incidents. Links to these documents are provided in the "Helpful Website" section of this Chapter.

Initial Reports:

HQ personnel must promptly report suspected Incidents of Security concern to AU-40, their respective HSO, or a protective force officer. The discovering organization's HSO normally performs the initial reporting, which may be done telephonically ensuring that only unclassified information is communicated unless a Secure Terminal Equipment (STE) or Viper is being used. If the initial report is made telephonically or verbally, it must be followed by a formal written initial report. Formal reporting can be accomplished by sending an unclassified/ encrypted e-mail. The notification e-mail **MUST** contain the word **Incident** in the subject line. The e-mail can attach a template, *Initial Report of a Headquarters Security Incident* (Attachment 11-1). If the template is not used, the information provided in the Initial Report must correspond to all fields in the template. Reports made in writing must be properly classified.

> ***CAUTION:*** *Details of security incidents may be classified. Consult with a classifier before preparing or submitting these messages.*

The HQ Security Incidents Program Manager (HSIPM) coordinates evaluation of and response to HQ incidents. After reviewing the suspected incident, the HSIPM determines whether it should be handled as an incident or an administrative matter.

> ***EXAMPLE:*** *Unless there was a compromise or aggravating circumstance (such as a repeat offense), failing to use a "Candy Stripe" envelope to carry classified matter within HQ should be handled as an administrative matter and the employee retrained, not as an Incident of Security Concern.*

> ***NOTE:*** *Incidents discovered, documented, and reported to AU-40 by the HQ Protective Force are usually considered Management Interest incidents and do not require additional reporting or official inquiries).*

Within 5 business days of being confirmed as an Incident, the HSIPM categorizes the incident in coordination with the reporting entity based on guidance contained in Attachment 5 to DOE Order 470.4B, Chg. 2. The Incident will be categorized as a Security Incident (SI), a Procedural Interest (PI), or an Item of Management Interest (MI). (See Attachment 11-2.)

Based on the information involved and the likelihood of compromise, the HSIPM, the program office reporting the incident, and AU-40 management are consulted to determine whether a Damage Assessment (DA) and/or Notification to Congress as a "Significant Nuclear Defense Intelligence Loss," per 50 U.S.C. Section 1656 is required.

> ***NOTE****: DAs and/or Notification to Congress may be required for confirmed or suspected compromises of Top Secret, SCI, SAP, and RD Nuclear Weapon Data. Weapon Data is Sigma 14, 15, 18, or 20 information as defined by DOE Order 452.8. The organization with programmatic responsibility for the information/material would handle the reporting requirements and conduct of the DA. Also see Section 1, Attachment 5 of DOE Order 470.4B, Change 2 for reporting guidance.*

The HSIPM ensures that all HQ Incidents of Security Concern categorized as an SI or PI are logged into SSIMS and assigned unique tracking numbers.

Assignment of Inquiry Official:

A formal documented inquiry to determine the facts and circumstances of the incident is required for all SI and PI incidents. The HSIPM assigns responsibility for performing inquiries to the designated organizational Inquiry Officer in the organization where the incident occurred. However, the HSIPM may assign an Inquiry Officer from a different organization to perform the inquiry if the organization doesn't have an Inquiry Officer or if the organization so requests.

Inquiry officers must meet the requirements of and be knowledgeable of Section 1, Attachment 5 to DOE Order 470.4B, Change 2, i.e., they must have previous investigative experience or Departmental Inquiry Official training and must be knowledgeable of appropriate laws, executive orders, Departmental directives, and/or regulatory requirements. Inquiry officers are appointed by their management based on the criteria above. Copies of appointment memoranda are provided to the HSIPM along with either a training certificate or description of investigative experience.

The HSIPM assigns the inquiry by memorandum to the appointed Inquiry Official or his/her designee requesting an inquiry be performed that states the details of the incident, provides associated documentation, and requests that a completed DOE F 5639.3, *Report of Security Incident/Infraction,* be provided with the inquiry closure report.

The inquiry officer's first priority is to ensure that appropriate action is taken to mitigate the incident, e.g., securing documents, sanitizing e-mail servers, etc. Once mitigating actions have been completed, the inquiry officer tries to determine the cause of the incident, what actions must be taken to address any underlying weaknesses, and recommend the appropriate follow up actions including retraining, issuance of a security infraction, or other disciplinary action.

Should the inquiry officer believe during the investigation that a criminal act may have occurred or that an agent of a foreign power is involved, the inquiry officer must immediately cease the inquiry and notify the HSIPM.

> ***NOTE:*** *Although inquiry officers may be Federal or contractor employees, only Federal employees are authorized to contact outside agencies/organizations (e.g., Postal Service; FBI; or Federal, State, or local agencies) in regard to an ongoing inquiry. Such contact should be coordinated with the HSIPM.*

Completed Category A incident reports must be submitted to the HSIPM within 90 days of assignment. If additional time is required, the HSIPM must be notified and an extension requested.

Inquiry/Closeout Reports:

A formal closeout report is required for all security incidents with the interest type of SI or PI. Templates for the most common security incidents may be used to help Inquiry Officers complete their reports and can be obtained from the HSIPM. Closeout Reports should remain unclassified if at all possible. If the Inquiry Officer chooses not to use the templates, he/she must create a report that details the following information:

- A full description of the incident (i.e., "who, what, where, why, when, and how") providing more detail than contained in the initial report.

- For all incidents, the report must include the name of the individual(s) primarily responsible for the incident, including a record of prior incidents for which the individual(s) had been determined responsible. Other involved individuals must also be named. Access authorization levels (for all individuals involved) must be clearly stated.

- The report must identify mitigating factors that reduce the potential impact of the incident (such as confirmation that affected computer systems were immediately sanitized) or any other action that reduces the potential impact of the incident.

- The report must identify aggravating factors that increase the potential impact of the incident (for example, a security container was left unsecured for an undetermined period of time).

- The report must identify any corrective actions that will be taken to preclude recurrence, including retraining, issuance of a security infraction, or other disciplinary action.

> ***NOTE:*** A copy of the DOE F 5639.3*, Report of Security Incident/Infraction* must be completed by the Inquiry Officer regardless if the responsible individual will or will not be issued an infraction. If it is determined that no infraction is warranted, the basis for that determination must be documented in the inquiry report. DOE F 5639.3 must be attached to the inquiry report and signed by the responsible individual's Office Director. Infractions can be issued to cleared and non-cleared individuals who violate security requirements.

For Information Protection incidents, the inquiry officer determines the likelihood of compromise per the definitions below:

- Loss/Compromise did Occur. Compromise was confirmed. Information was disclosed to an unauthorized person(s) (e.g., published by media, briefed to unauthorized individuals, etc.).

- Probability of Compromise is not Remote. Compromise is suspected. Lacking a clear indication of compromise (i.e., no direct recipient), the circumstances are such that there is an obvious possibility of unauthorized disclosure (e.g., classified information is transmitted by e-mail outside of the organization's firewall, classified information is communicated on an unsecure phone line, etc.).

- Probability of Compromise Is Remote. A low possibility exists that information was disclosed to unauthorized personnel (e.g., classified information is left unsecured and unattended for a limited amount of time in an area accessed only by personnel with the appropriate clearance level, classified information is transmitted by e-mail inside the organization's firewall and is discovered and isolated within a specified period of time).

- Loss/Compromise Did Not Occur. No possibility of compromise exists (e.g., although an open storage area was not secured, the access control system shows the door was not opened).

For example, when determining the extent of compromise the following table should be used:

Likelihood Of Compromise Guidelines Non-Secure Transmittal of Classified Matter Over Electronic Networks (i.e., e-mail)	
Circumstances of the non-secure transmittal	**Likelihood of Compromise is:**
Any addressee is uncleared to have received the information	Confirmed
Transmittal within the firewall, encrypted and sanitized within 24 hours	Remote
Transmittal within the firewall, not encrypted and sanitized within 8 hours	Remote
For all other transmittals	Is not Remote

For any confirmed or suspected compromise as mentioned above, the extent of dissemination (e.g., number of individuals and their citizenship; global disclosure via cyber media; open source publication; etc.) should be identified.

If applicable, a determination is made as to whether an unauthorized disclosure was willful (i.e., intentional vs. inadvertent disclosure).

Incident Closure:

The HSIPM reviews the inquiry report to ensure that it is complete and adequately addresses date of occurrence, individuals involved, cause, actions to contain incident, corrective actions and actions to prevent recurrence.

When all requirements of closure are met, the HSIPM has the SSIMS database updated. He/she distributes the report, and files the DOE F 5639.3 with DOE Personnel Security and AU-40 management.

Tracking and Trending:

Each security incident must be assigned a tracking number by the HSIPM. The HSIPM is responsible for maintaining a spreadsheet that contains a tracking number and additional information to include the incident date, category, incident type, HSO or Inquiry Official, completion date, and whether or not the incident resulted in disciplinary action, such as a security infraction. (Organizational elements at Headquarters may also maintain their own local tracking number to track/trend their incidents should they choose to do so.)

The HSIPM will provide the Director, Office of Physical Protection, with information from the spreadsheet for the purpose of monitoring security program performance and to gauge deficiencies where site security procedures may need to be modified or whether corrective actions need to take place to enhance Headquarters' security posture.

Retention of Files:

The HSIPM maintains a 5-year history file of HQ security incidents in accordance with RIDS requirements. Additional incident records are maintained in the SSIMS database.

Points of Contact

For the names and contact information for the positions identified in this chapter, call (301) 903-2644 or (301) 903-7189.

Forms/Samples/Graphics

Template for Initial Report of a Headquarters Security Incident (see Attachment 11-1)

Incident Categories and Types (see Attachment 11-2)

Template for appointment of an Inquiry Officer (see Attachment 11-3).

Helpful Website

DOE Order 470.4B, Change 2, *Safeguards and Security Program, Attachment 5 Incidents of Security Concern.* https://www.directives.doe.gov/directives-documents/400-series/0470.4-BOrder-B-Chg2-MinChg/@@images/file

DOE F 5639.3, *Report of Security Incident/Infraction,* https://energy.gov/sites/prod/files/cioprod/documents/5639-3.pdf

Inquiry officer training is available at: https://ntc.doe.gov/

DOE Standard Incidents of Security Concern, DOE-STD-1210-2012, September 2012, https://www.standards.doe.gov/standards-documents/1200/1210-astd-2012/@@images/file

ATTACHMENT 11-1
(Template) Initial Report of a Headquarters Security Incident

When document is completed please mark as OUO

Date of Discovery	Time of Discovery	Place of Discovery	Incident Number
Local Tracking Number (if used)			

	Incident Topical Area	Type (MI/SI/PI)	Category (A/B)
□	Information Protection (Complete "Supplement" section below)		
□	Protective Force		
□	Physical Security		
□	Program Management		
	Are Foreign Nationals Involved? (Check Yes or No.)	□ Yes	□ No
	Is Media Interest likely? (Check Yes or No.)	□ Yes	□ No

Brief **UNCLASSIFIED** Description of Incident. (Classified details, if needed, must be sent separately.)

CAUTION – Details of Security Incidents may be classified – Check with a Classifier before completing.

Describe the initial steps taken to mitigate the incident.

Supplement for Information Protection Incidents

What is the highest level and category of Information involved?

Classification Level	□ Top Secret	□ Secret	□ Confidential
Classification Category	□ RD	□ FRD	□ NSI

Do any Special Caveats apply? (Check all that apply)

WD*	SCI	SAP	WFO	FGI	OGA	NOFORN	Other:
□	□	□	□	□	□	□	

*WD, Weapon Data, is information in Sigma 14, 15, 18 or 20 as defined by DOE O 452.8.

For Controlled Unclassified Information (CUI) – insert type	
What organization has programmatic responsibility for the information?	

Program Office and HSIPM Determinations

Does the incident constitute a, "Significant Nuclear Defense Intelligence Loss," requiring Congressional Notification per 50 U.S.C. Section 2656?	Yes □	No □
Is a formal Damage Assessment warranted?	Yes □	No □

Point of Contact (Person Making Report)

Name	Title	Organization	Phone

ATTACHMENT 11-2
Incident Categories and Types

Topical Area	PMS		PF			PSS				NMCA				IP			
Interest Type	MI		SI	PI		SI		PI		SI		PI		SI		PI	
Category	A	B	A	A	B	A	B	A	B	A	B	A	B	A	B	A	B
Incident Type																	
Arrest	◆																
On-Site Arrest	◆	◆															
Degradation of Security	◆																
Hostile Act	◆																
Investigation	◆																
Labor Strike	◆																
Media Event	◆																
Suspicious Activity	◆																
Threats	◆																
Confiscated Firearm	◆																
Demonstrations/Protest	🔷	◆															
Non-Willful Intrusion		◆															
Loss			◆			◆	◆			◆				◆	◆		
Theft			◆			◆	◆			◆				◆	◆		
Unauthorized Discharge				◆													
Improper Storage					◆									◆			◆
Unauthorized Introduction of Prohibited Articles						🔷		🟩	◆								
Improper Access Control		◆							◆								
Unauthorized Introduction of Controlled Articles						🔷		🟩	◆					◆			◆
Process Difference										◆	◆						
Inventory Difference										◆	◆						
Shipper Receiver Difference										◆	◆						
Unauthorized Movement												◆					
Improper Handling										🔷		🟪	◆				◆
Cyber Attack that Compromises the Unclassified Network															🔷		
Cyber Incident Resulting in Compromise of Information														◆	◆		
Processing Information on an Unapproved Computer System														◆	🟩		🔷
Unauthorized Network Based Transmission of Information														◆	◆		◆
Unauthorized Recipient of Information														◆	🟩		🔷
Transmission of Information on an Unauthorized Communication System														◆	🟪		🔷
Oral/Visual														◆			◆

🔷 - New Incident Categorization
🟩 - Categorization no longer valid as of 05/26/2015, incidents prior to 05/26/2015 may still use these.
🟪 - Categorization removed

Category A – Incidents that meet a designated level of significance relative to the potential impact on the Department and/or national security, thereby requiring the notification and pertinent involvement of DOE/NNSA cognizant security office (CSO) and the contractor CSO.

Category B – Incidents of lesser significance that are managed and resolved by the contactor CSO. However, oversight responsibilities remain with the DOE/NNSA CSO.

ATTACHMENT 11-3

Date

MEMORANDUM FOR (INQUIRY OFFICIAL NAME AND TITLE HERE)

FROM: (NAME OF OFFICE DIRECTOR AND TITLE HERE)

SUBJECT: Appointment as Inquiry Official

Based on your prior experience and/or formal training in the Headquarters Inquiry Program, I am appointing you as an Inquiry Official in accordance with the requirements of Attachment 5 to Department of Energy (DOE) Order 470.4B, Safeguards and Security Program.

As an Inquiry Official, you are authorized to conduct inquiries into specific security incidents as assigned by me or by our office's Headquarters Security Officer. As assigned, you are to determine the facts and circumstances of security incidents(s), identify who was responsible for them, and draw specific conclusions on the potential for compromise of classified or sensitive information. You are authorized to conduct interviews, review and copy records, and perform other actions required for a thorough review of these incidents. You may present this memorandum to anyone who may desire confirmation of your authority to perform security inquires.

This memorandum certifies to all departmental personnel that you have "need to know" for all information related your appointment as an inquiry official consistent with your access authorities.

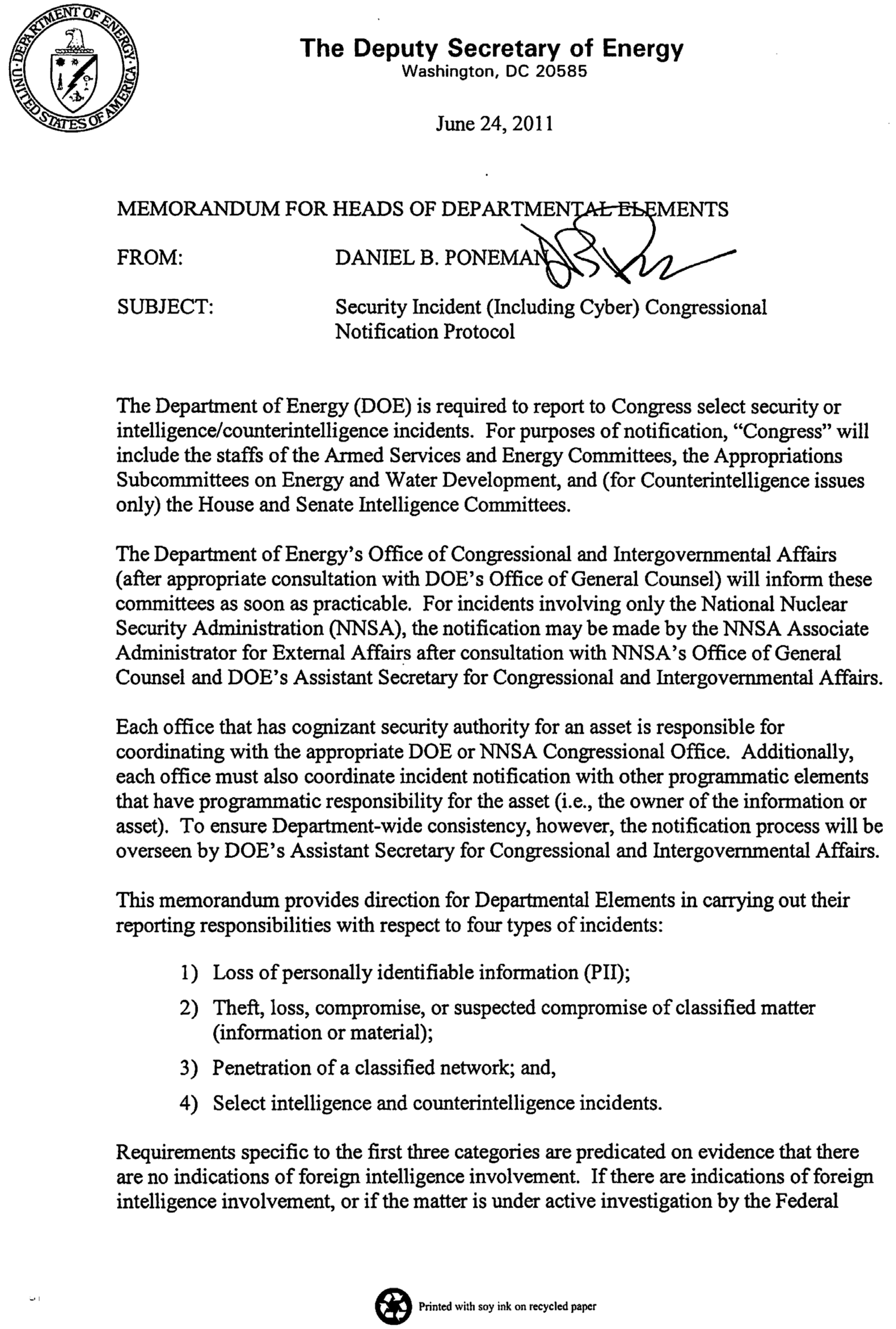
You may conduct security inquires by yourself or use a team approach. If you opt to use the latter, you are responsible for ensuring all team members meet DOE requirements and are knowledgeable of their roles, responsibilities, and limitations to ensure the legal aspects of inquiries are not violated.

cc:
Ruth Watkins, AU-40

ATTACHMENT 11-4

Deputy Secretary of Energy Memorandum, Security Incident (Including Cyber) Congressional Notification Protocol, June 24, 2011

For



The Deputy Secretary of Energy
Washington, DC 20585

June 24, 2011

MEMORANDUM FOR HEADS OF DEPARTMENTAL ELEMENTS

FROM: DANIEL B. PONEMAN

SUBJECT: Security Incident (Including Cyber) Congressional Notification Protocol

The Department of Energy (DOE) is required to report to Congress select security or intelligence/counterintelligence incidents. For purposes of notification, "Congress" will include the staffs of the Armed Services and Energy Committees, the Appropriations Subcommittees on Energy and Water Development, and (for Counterintelligence issues only) the House and Senate Intelligence Committees.

The Department of Energy's Office of Congressional and Intergovernmental Affairs (after appropriate consultation with DOE's Office of General Counsel) will inform these committees as soon as practicable. For incidents involving only the National Nuclear Security Administration (NNSA), the notification may be made by the NNSA Associate Administrator for External Affairs after consultation with NNSA's Office of General Counsel and DOE's Assistant Secretary for Congressional and Intergovernmental Affairs.

Each office that has cognizant security authority for an asset is responsible for coordinating with the appropriate DOE or NNSA Congressional Office. Additionally, each office must also coordinate incident notification with other programmatic elements that have programmatic responsibility for the asset (i.e., the owner of the information or asset). To ensure Department-wide consistency, however, the notification process will be overseen by DOE's Assistant Secretary for Congressional and Intergovernmental Affairs.

This memorandum provides direction for Departmental Elements in carrying out their reporting responsibilities with respect to four types of incidents:

1) Loss of personally identifiable information (PII);
2) Theft, loss, compromise, or suspected compromise of classified matter (information or material);
3) Penetration of a classified network; and,
4) Select intelligence and counterintelligence incidents.

Requirements specific to the first three categories are predicated on evidence that there are no indications of foreign intelligence involvement. If there are indications of foreign intelligence involvement, or if the matter is under active investigation by the Federal

Bureau of Investigation (FBI), reporting will be handled by DOE's Office of Intelligence and Counterintelligence, consistent with category 4, above, in consultation with the FBI and Department of Justice.

Loss of personally identifiable information (PII) in electronic form or hardcopy for 100 or more individuals. "Loss" will mean disclosure outside of the Federal Government or its contractors. Inadvertent access by a Federal or contractor employee to PII to which he or she would not normally be authorized access, or the unencrypted emailing of PII that does not suggest any possibility of compromise, will not be considered "loss" for purposes of this protocol and need not be reported. For PII incidents within DOE, the "incident" office shall notify the DOE Chief Information Officer, who will notify the DOE Office of Congressional and Intergovernmental Affairs. For PII incidents within NNSA, the "incident" office shall notify the NNSA Chief Information Officer, who will then notify the Chief of Defense Nuclear Security, the Principal Deputy Administrator, the Administrator, and the NNSA Associate Administrator for External Affairs. The NNSA Associate Administrator for External Affairs will have the responsibility to notify Congress and other appropriate parties.

Theft, loss, compromise, or suspected compromise of classified matter (information or material). Incidents involving the theft, loss, compromise, or suspected compromise of Top Secret, Sensitive Compartmented Information, Special Access Program, or Restricted Data Weapons Data information must be reviewed by the office with programmatic responsibility for the information. This review is to determine if it constitutes a "significant nuclear defense intelligence loss" (i.e., likely to cause serious harm or damage to the national security interest of the United States as defined in Executive Order 13526, *Classified National Security Information*).

Incidents requiring the notification of Federal line management that involve the theft or loss of physical assets (e.g., special nuclear material, classified weapons components/parts, etc.) must be assessed by the cognizant program office to determine if the details of the incident constitute a risk or threat to national security.

As specified in 50 U.S.C. 2656, *Notice to Congressional Committees of Certain Security and Counterintelligence Failures within Nuclear Energy Defense Programs,* the Department must, after consultation with the Director, Central Intelligence Agency, and the FBI Director, as appropriate, provide notification to Congress within 30 days after the date on which the Department determines that the loss has taken place. For NNSA-specific issues, the Chief of Defense Nuclear Security will report through the NNSA Associate Administrator for External Affairs. For non-NNSA issues, the Cognizant Program Office will report after consultation with the DOE Office of Congressional and Intergovernmental Affairs.

Penetration of a classified network. For actual or suspected penetration of DOE classified networks, the DOE Chief Information Officer will notify the Office of Congressional and Intergovernmental Affairs and the Department's Chief Health, Safety and Security Officer. For actual or suspected penetration of NNSA classified networks, the NNSA Chief Information Officer will notify NNSA's Associate Administrator for

External Affairs, the Chief of Defense Nuclear Security, and both the Principal Deputy Administrator and Administrator.

Certain Intelligence and Counterintelligence incidents. For significant incidents as described by categories 1 through 3 and for which there is also a foreign intelligence nexus, reporting responsibility resides with DOE's Office of Intelligence and Counterintelligence, under Director of National Intelligence guidelines.

In each instance where there is doubt as to whether an issue should be reported, the issue will be resolved in favor of reporting. Concurrent with notifications to DOE's Office of Congressional and Intergovernmental Affairs, all Departmental Elements should simultaneously notify NNSA Office of Public Affairs (for NNSA-specific issues) and the DOE Office of Public Affairs (for both DOE and NNSA issues) for the appropriate determination of media applicability.

This policy shall be reviewed annually in June for continued relevance.

cc: Robert Osborn II, NA-2.2
Bradley Peterson, NA-70
Theodore Wyka, Jr., NA-71
Reece Edmonds, NA-711
Glenn Podonsky, HS-1
Michael Locatis, DOE, CIO