

Chapter 11

Incidents of Security Concern

This chapter covers the DOE HQ implementation of DOE Order 470.4B, *Safeguards and Security Program, Attachment 5, Incidents of Security Concern*. AU-41 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
- 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 that 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 that corrective actions to mitigate the incident are taken.
- Develop actions to correct underlying weaknesses and prevent recurrence.
- Document whether a security infraction or other disciplinary action is needed.

HQ Implementation Procedures

Initial Reporting:

HQ personnel must promptly report suspected Incidents of Security Concern to AU-41. The discovering organization's HSO normally performs the initial reporting, which may be done verbally. However, any concerned individual may contact a protective force officer or AU-41 staff to report suspected incidents.

The HQ Security Incidents Program Manager (HSIPM) coordinates evaluation of and response to HQ incidents.

After reviewing the suspected incident, the HSIPM determines whether the suspected incident rises to the level of an Incident or if it is better handled as 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.*

Within three business days of being confirmed as an Incident, it must be categorized as either a Security Incident (SI) or an Item of Management Interest (MI). SIs are further sub-categorized as Information Protection (IP), Protective Force/Executive Protection (PF), or Physical Security (PS) incidents (see Attachment 1100-1).

NOTE: *DOE O 470.4B establishes a third category, items of Procedural Interest (PI). Because SI and PI incidents have the same follow-up, the two categories are merged in the HQ program. Similarly, as there is no separate contractor security organization, the HQ implementation does not differentiate between Category A and B incidents.*

Once categorized, incidents must be formally reported to AU-40. Formal reporting is accomplished by sending an UNCLASSIFIED/ENCRYPTED e-mail to AU-40’s **HEADQUARTERS SECURITY OPERATIONS** mailbox.

The notification e-mail **MUST**:

- Contain the word **Incident** in the subject line.
- Identify the time, date, and place of incident discovery.

NOTE: *Time and date of discovery is not the same as time and date of occurrence.*

- Identify incident category (SI or MI) and SI subcategory (IP, PF, or PS) per Attachment 1100-1.
- Indicate whether foreign nationals were involved.
- Indicate whether media interest is likely.
- Include an **UNCLASSIFIED** description of the incident.
- Indicate the initial steps taken to mitigate the incident (i.e., all classified matter has been secured, unauthorized personnel have been escorted out of the area, etc.).
- For IP incidents, the initial report must also identify the level and category of information and any caveats or special handling requirements.

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

NOTE: *Incidents discovered, documented, and reported by the HQ Protective Force to AU-41 do not require the additional reporting (as described above).*

To help meet these requirements, an *Initial Report of Headquarters Security Incident* template has been developed (see Attachment 1100-2).

Formal notification should be followed up with a telephone call to the HSIPM.

Based on the information involved and the likelihood of compromise, the HSIPM and program office 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 TS, SCI, SAP, and RD Nuclear Weapon Data. Weapon Data is Sigma 14, 15, 18, or 20 information as defined by DOE Order 452.8 (see Attachment 1100-3).*

HSIPM coordinates additional reporting, which is required for incidents anticipated to be reported in the media or involving non-U.S. citizens.

HSIPM ensures that all HQ Incidents of Security Concern are logged into SSIMS and assigned unique tracking numbers.

Follow-Up Activities:

No additional action is required for MI incidents.

An inquiry to determine the facts and circumstances of the incident is required for all SI incidents. The HSIPM assigns responsibility for performing inquiries. Usually, responsibility is assigned to the HQ element where the incident occurred; however, the HSIPM may assign responsibility elsewhere.

Assignment shall be by memorandum or e-mail. The assignment document shall provide copies of the original reporting documents, and a partially completed DOE F 5639.3, *Report of Security Incident/Infraction*.

The responsible HQ element assigns an inquiry officer to investigate the incident. Inquiry officers must meet the requirements of Attachment 5 to DOE Order 470.4B, 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. Copies of appointment memoranda are provided to the HSIPM.

Inquiries are performed in accordance with Attachment 5 to DOE Order 470.4B. When the inquiry officer believes 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.

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.

For IP incidents, the inquiry officer determines the likelihood of compromise per the definitions below (see also the guidelines for non-secure transmittals of classified information, below):

- **Compromise Confirmed.** Information was disclosed to an unauthorized person(s) (e.g., published by media, briefed to unauthorized individuals, etc.).
- **Compromise 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.).
- **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).
- **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).

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	Suspected

DAs, when required, shall consider the value of the information, to whom the information would be valuable, and whether the information was previously compromised. A suggested model for determining level of damage for nuclear weapon design information follows.

Damage Assessment Guidelines (Nuclear Weapon Information)		
Information Value	Interested Adversaries	Previously Compromised
Critical/keystone data (5)	First time proliferant (3)	No (2)
Helpful but non-essential data (3)	Technically sophisticated non-weapons state (2)	Perhaps (1)
Minor technical detail (1)	Existing nuclear weapons state (1)	Appears in open literature (0)

The scores in the three areas are multiplied and the damage assessed as High (over 20), Moderate (10-20), or Low (less than 10). DAs for incidents involving other information are based on similar criteria, and the basis included in the closeout report.

Closeout Reports:

A closeout report is required for all security incidents (IP, PF, or PS). The report must include:

- A full description of the incident (i.e., the “who, what, when, and where”) filling blanks left in the initial report
- 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
- A statement of actions taken to mitigate the incident
- A statement of actions taken to preclude recurrence, including retraining, issuance of a security infraction, or other disciplinary action.

NOTE: *If an infraction is issued, Part II of the DOE F 5639.3, Report of Security Incident/Infraction, must be completed and the necessary approvals obtained. A copy of the DOE F 5639.3 must be attached to the closeout report. If it is determined that no infraction is warranted, the basis for that determination must be documented in the report.*

For IP incidents, the report must also address:

- The inquiry officer’s determination of the likelihood of a compromise and the basis for that determination
- For any confirmed or suspected compromise, the extent of dissemination (e.g., number of individuals and their citizenship; global disclosure via cyber media; open source publication; etc.)
- If a DA was required, the level of damage and the basis for the damage determination
- If applicable, a determination as to whether an unauthorized disclosure was willful (i.e., intentional vs. inadvertent disclosure)

- Identification of any collateral effect (i.e., extent of condition) on other programs or security interests.

Completed 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.

Worksheets are available to assist in the preparation of inquiry reports for some of the more common incidents, such as failure to secure a classified repository, classified information included in a non-secure e-mail, etc. Inquiry Officers may contact the HSIPM to check on availability of appropriate worksheets.

Incident Closure:

The HSIPM reviews the inquiry report to ensure that it is complete and adequately addresses cause, corrective action, and action to prevent recurrence.

When all requirements are met, the HSIPM has the SSIMS database updated and distributes the report and any associated DOE F 5639.3, as necessary.

The HSIPM maintains a five 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 (202) 586-8075 or (301) 903-2644.

Forms/Samples/Graphics

Incident Categories and Types (see Attachment 1100-1)

Template Initial Report of a Headquarters Security Incident (see Attachment 1100-2)

Deputy Secretary of Energy Memorandum, Security Incident (Including Cyber) Congressional Notification Protocol, June 24, 2011 (see Attachment 1100-3)

Helpful Website

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

ATTACHMENT 1100-1

Incident Categories and Types

INFORMATION PROTECTION INCIDENTS (Category SI)	
Incident Description	Type
Loss, theft or <u>confirmed</u> compromise of classified information	IP-1
Failure to Protect Classified Matter (See below)	IP-2
Failure to secure a vault or vault type room	IP-2.1
Failure to secure a classified repository	IP-2.2
Unattended classified matter	IP-2.3
Classified information processed on a system not accredited for the level and category of information	IP-2.4
Classified information transmitted over a system not accredited for the level and category of information	IP-2.5
Classified information discussed in an area not approved for the level and category of information	IP-2.6
Other acts which create a <u>substantive</u> risk of compromise of classified matter. NOTE: Risk must be substantive to be treated as an incident. For example, absent aggravating circumstances (such as a repeat offense), failing to use a "Candy Stripe" envelope to carry classified matter within Headquarters should be handled as an administrative matter and the employee retrained, not as an IOSC.	IP-2.7
Loss, theft or <u>confirmed</u> compromise of CUI matter	IP-3
Failure to Protect CUI Matter (See Below)	IP-4
Failure to store CUI matter in accordance with DOE Directives	IP-4.1
Failure to transmit CUI matter in accordance with DOE Directives	IP-4.2
Other acts which create a <u>substantive</u> risk of compromise of CUI matter NOTE: Risk must be substantive to be treated as an incident. For example, absent aggravating circumstances (such as a repeat offense), failing to mark an envelope "For Addressee Only" should be handled as an administrative matter, corrected and the employee retrained, not as an IOSC.	IP-4.3
Other Information Protection incident(s) warranting formal logging and follow up	IP-5

PROTECTIVE FORCE/EXECUTIVE PROTECTION INCIDENTS (Category SI)	
Incident Description	Type
Theft or loss of a firearm; theft or loss of ammunition in excess of DOE 0 473.3 requirements	PF-1
Theft or loss of an armored vehicle	PF-2
Improper storage of firearms or ammunition	PF-3
Unintended discharge of a firearm	PF-4
Other Protective Force/Executive Protection incident(s) warranting formal logging and follow up	PF-5

PHYSICAL SECURITY INCIDENTS (Category SI)	
Incident Description	Type
Theft or loss of security keys which permit <u>undetected</u> access to a headquarters facility, security area or classified matter repository	PS-1
Loss, theft or willful destruction of Government property in excess of \$25,000	PS-2
Accidental (including weather related) destruction of Government property in excess of \$100,000	PS-3
Unauthorized introduction of Prohibited Items (including alcoholic beverages) into the a headquarters PPA	PS-4
Unauthorized introduction of Controlled Items (including alcoholic beverages) into an LA or above	PS-5
Failure to properly escort uncleared personnel in security areas	PS-6
Failure to properly escort visitors (US or foreign nationals) during security hours	PS-7
Failure to register foreign visitors/assignees in FACTS per DOE Directive requirements or Foreign Nationals gaining access a Headquarters PPA without proper authorization	PS-8
Issue of a badge reflecting a higher level of access than the individual is authorized	PS-9
Theft (vs. loss) of a DOE security badge where the badge was the target of the theft	PS-10
Willful entry into a Security Area (LA or above) without proper authority	PS-11
Other Physical Security/Program Planning and Management Incident(s) warranting logging and follow up	PS-12

ITEMS OF MANAGEMENT INTEREST (Category MI)	
Incident Description	Type
Non-willful intrusions into Security Areas (LA or above)	MI-1
Intrusions into Property Protection Areas	MI-2
Interaction with Law Enforcement resulting in detention or a fine in excess of \$250	MI-3
Investigation or official inquiry of an employee (Federal or Contractor) pertaining to a criminal felony	MI-4
Hostile acts or threats of hostile acts against headquarters property or facility likely to cause damage	MI-5
Hostile acts or threats of hostile acts against headquarters personnel either occurring at work or for reasons related to their employment	MI-6
Suspicious Activity, including surveillance of a headquarters facility	MI-7
Peaceful demonstrations or protests involving more than 20 participants	MI-8
Labor strike or threat of a strike impacting HQ's security posture	MI-9
Degradations of Security	MI-10
Any Security related occurrence that results in media questions	MI-11
Protective Forces Officer required to use force to control a situation	MI-12
Other Physical Security/Program Planning and Management Incident(s) warranting formal logging (but no follow up)	MI-13

ATTACHMENT 1100-2
(Template) Initial Report of a Headquarters Security Incident

Discovery Date	Discovery Time	Place of Occurrence	Local Number (If applicable)	Incident Number (Assigned by HSIPM)
Incident Category and Type (Check applicable row and fill in type number)				Category Type
Information Protection (Complete supplementary section below)				SI IP -
Protective Force/Executive Protection				SI PF -
Physical Security				SI PS -
Item of Management Interest				MI MI -
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
*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	Organization	Phone

OFFICIAL USE ONLY (When Filled In)

May be exempt from public release under the Freedom of Information Act (5 U.S.C. 552), exemption numbers and categories: (6) Personal Information, (7) Law Enforcement. Department of Energy review required before public release.

Name/Org: _____ Date: _____ Guidance: CG-SS-4, September 2000

Official Use Only (When Filled In)

ATTACHMENT 1100-3

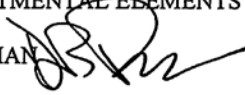
Deputy Secretary of Energy Memorandum, Security Incident (Including Cyber) Congressional Notification Protocol, June 24, 2011



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



Printed with soy ink on recycled paper

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