Chapter 11 Revision History as of 07/03/2023:

July 3, 2023: Updated organization name and abbreviation. Additional revisions under "Initial Reporting" section.

August 12, 2022: Revised revision history, formatting, and hyperlinks.

November 22, 2019: Sections on identifying and categorizing incidents and tracking and trending has been added. A fillable form "Initial Report of Headquarters Security Incident" was created.

January 5, 2018: This entire chapter has undergone a major revision. As changes are too extensive to itemize, please review Chapter 11 in its entirety.

Chapter 11
Incidents of Security Concern

This chapter covers the DOE HQ implementation of DOE Order 470.4B, Chg. 3, *Safeguards and Security Program,* Attachment 4*, Incidents of Security Concern*. The Office of Headquarters Security Operations (EHSS-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, Chg. 3, *Safeguards and Security Program,* Attachment 4*, Incidents of Security Concern*, and provides greater detail on incident categorization and incident criteria. An Incident Categorization Matrix has been developed to assist with identification and categorizing of Incidents based on the type of incident event and is provided within this chapter.

DOE Standard Incidents of Security Concern, DOE-STD-1210-2012, September 2012, contains additional information and guidance on identifying and categorizing security incidents. Links to these documents are provided in the "Helpful Website" section of this Chapter.

Initial Reporting:

HQ personnel must promptly report suspected incidents of security concern to their respective Headquarters Security Officer (HSO), or a Contractor Protective Force (CPF) officer. CPF will notify the HSIPM of a possible security concern. The HSIPM will alert the HSO of the program office involved.

The discovering organization's HSO will perform the initial reporting to the HQ Security Incidents Program Manager (HSIPM), 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 to, HQIOSCProgram@hq.doe.gov The notification e-mail **MUST** contain the word **Incident** in the subject line. The e-mail should include the *Initial Report of a Headquarters Security Incident*. 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.*

If a potential incident crosses multiple program or staff office jurisdictions, then the office that suspects that the security incident occurred must take primary responsibility and execute the necessary reporting and notification processes. 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.*

Incident Identification and Categorization

Within 5 calendar days of being confirmed as an Incident, the HSIPM categorizes the incident in coordination with the reporting entity based on guidance contained in Attachment 4 to DOE Order 470.4B, Chg. 3. The Incident will be categorized as:

Category A: Incidents, which meet a designated level of significance relative to the potential impact on the Department and/or national security, require the notification of the DOE/NNSA CSO and the contractor CSO. The involvement of the DOE/NNSA CSO for Category A incidents is imperative for assessing impacts, coordinating with external agencies, and/or notifying senior management.

Category B: Do not meet the Category A criteria, are managed, and resolved by the contractor CSO; however, this does not preclude the DOE/NNSA CSO from exercising its oversight responsibilities.

Incident Type:

- Security Incident (SI),
- Procedural Interest (PI)
- Management Interest (MI)

If there is still uncertainty at the 5-calendar day mark, with respect to incident categorization, the incident must be reported as a Category A pending completion of the inquiry process. If the final inquiry reveals additional details and facts, the incident can be re-categorized.

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

Based on the information involved and the likelihood of compromise, the HSIPM, the program office reporting the incident, and EHSS-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 4 of DOE Order 470.4B, Change 3, for reporting guidance.*

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. Once the reporting element designates an Inquiry Officer from within their organization, the HSIPM formally assigns responsibility for performing the inquiries by memorandum that states the details of the incident and provides associated documentation. 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 by request of the reporting organization.

Inquiry officers must meet the requirements of and be knowledgeable of Section 1, Attachment 4 to DOE Order 470.4B, Change 3, i.e., they must have previous investigative experience or Departmental Inquiry Official training through the DOE National Training Center, Learning Nucleus site; *PMC-300DE, Legal Aspects Overview, and the PMC-310, Incidents of Security Concern Fundamentals.* The individual 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 inquiry officer's 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) regarding 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 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).

- 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.

  A copy of the DOE F 5639.3, *Report of Security Incident/Infraction* must be completed by the Inquiry Officer. 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 timeframe).

- 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, if applicable. The report is distributed with a copy of the DOE F 5639.3 to DOE Personnel Security and EHSS-80 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 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) 903-0885.

Forms/Samples/Graphics

Initial Report of a Headquarters Security Incident – fillable pdf

Incident Categories and Types

Sample Memo – Appointment as Inquiry Officer

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

Helpful Websites

DOE Order 470.4B, Chg. 3, *Safeguards and Security Program,* Attachment 4*, Incidents of Security Concern*

DOE F 5639.3, *Report of Security Incident/Infraction*

Inquiry officer training is available at: National Training Center

DOE Standard Incidents of Security Concern, DOE-STD-1210-2012, September 2012