# Chapter 8
# Operations Security Program

This chapter covers the OPSEC Program in place at DOE HQ to fulfill the requirements of DOE Order 471.6, Section 4.f, *Information Security Manual.*

The goal of the OPSEC Program is to assist HQ elements in identifying and protecting their Critical Information (CI) from inadvertent and unauthorized disclosure and assisting in the protection of classified information. CI includes those classified or sensitive unclassified areas, activities, functions, data or information about an activity or organization deemed important to protect from an adversary. CI, if disclosed, would have a negative impact on national security and/or departmental operations if unauthorized disclosure should occur. Examples of CI are personnel files (personally identifiable information (PII)), proposal and contract documents, and financial data regarding a project. CI is supported by indicators that are clues or paths that, when analyzed or combined, could lead an adversary to items contained in the CI. The HQ OPSEC Program provides senior managers with information to make sound risk management decisions concerning the protection of their sensitive information and ensures that OPSEC techniques and measures are implemented throughout HQ.

## HQ Implementation Procedures

### OPSEC Appointments:

The Director, Office of Headquarters Security Operations (AU-40), is responsible for appointing, in writing, a HQ OPSEC Program Manager.

The head of each element is responsible for appointing, in writing, both a primary and alternate OPSEC Representative. The primary and alternate OPSEC Representatives must possess a "Q" or "L" clearance and should be selected from positions normally included in policy decision making. The appointment memorandum should be formatted and addressed as described in the *Sample Appointment Memorandum* included in the Forms/Samples/Graphics subsection below. The head of each element must update the appointment memorandum each time there is a change to their OPSEC Representatives.

### HQ OPSEC Program Manager:

The HQ OPSEC Program Manager is responsible for all aspects of the program, including:

- Ensuring that OPSEC techniques and measures are used throughout HQ.
- Assisting HQ elements in identify their CI.
- Developing and executing an OPSEC awareness program that includes regular briefings to ensure that personnel are aware of their responsibilities in support of the OPSEC

program. These briefings may be integrated into, or provided in conjunction with, required security briefings (e.g., initial security briefings, comprehensive and/or annual security refresher briefings) and related meetings and workshops throughout the HQ.

- Assisting in OPSEC assessments of HQ elements to ensure that CI is being protected, element personnel are aware of their responsibilities for protecting CI, and ensuring that element leaders are aware of assessment results.

- Act as a technical advisor and expert on all matters affecting the HQ OPSEC program.

- Assign and document approved responsibilities for OPSEC direction, management, and implementation throughout the HQ.

## Element OPSEC Representatives:

The HQ OPSEC Representative is responsible for all aspects of their element's OPSEC program, including:

- Ensure appropriate and consistent implementation of current and newly developed OPSEC procedures throughout their area of responsibility.

- Make certain that employees in their element are aware of their OPSEC responsibilities and that they make OPSEC a part of their daily activities.

- Review information generated by or for the Federal Government being placed on any website or made available to the public to ensure it does not contain CI.

- Internally coordinate and develop the CI for their element.

- As is necessary, prioritize and update their element's CI and ensure it reflects current assets, threats, operations and other relevant factors. Submit the information to the HQ OPSEC Program Manager in a timely manner.

- Participate in HQ OPSEC assessments conducted within their element and brief their element leaders on the results of the assessment.

- Ensure corrective measures to mitigate vulnerabilities identified during OPSEC assessment are implemented expeditiously.

- Document and share the results of OPSEC assessments within their element.

- Routinely check offices to ensure there are no OPSEC vulnerabilities, i.e. computer screens unlocked, PII posted in plain view in unattended offices, CUI material in waste baskets and recycle bins (all are common OPSEC vulnerabilities).

- Maintain OPSEC Program data and ensure it is current. Program data should include, but is not limited to, current appointment memos, pertinent OPSEC directives, assessments/ reviews, and actions taken to enhance the element's OPSEC Program.

### OPSEC Assessments:

OPSEC assessments are conducted periodically to ensure that CI holdings are not inadvertently made available to unauthorized personnel. These assessments may be conducted as part of an OPSEC assessment or included in a HQ Survey Team survey/review. Results must be documented and shared with the element/site being assessed. It is important for the element's OPSEC Representative to be an active participant in these actions. The results of OPSEC assessments should be documented and shared with interested stakeholders such as the HQ Foreign Visits and Assignments Team, security program managers, and senior officials within the element.

It is recommended that an OPSEC assessment of sensitive activities and facilities be conducted when one or more of the following criteria arise:

- New construction is planned for a facility that will process or store classified or sensitive information.
- New sensitive activities are initiated or significant changes occur to existing programs.
- The element sponsors unclassified FV&As to HQ facilities.

### Information on Publicly Posted Websites:

Each HQ element must review information before it is posted to his/her publicly accessible websites to ensure it does not contain CI. The review must ensure the information does not place at unacceptable risk national security, DOE personnel and or assets, mission effectiveness, or the privacy of individuals. The element should periodically review published information to confirm appropriateness and continued compliance with DOE directives.

## Points of Contact

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

## Forms/Samples/Graphics

Sample Appointment Memorandum (see Attachment 800-1)

## Helpful Website

https://powerpedia.energy.gov/wiki/Operations_security

ATTACHMENT 800-1

***Sample Appointment Memorandum***

MEMORANDUM FOR (NAME), DIRECTOR
OFFICE OF HEADQUARTERS SECURITY OPERATIONS
OFFICE OF HEALTH, SAFETY AND SECURITY

FROM: (NAME)
NAME OF ELEMENT

SUBJECT: Appointment Memorandum for (Enter name of organization)

This memorandum notifies you of the (enter name of element) employees appointed to the following security-related positions:

Headquarters Security Officer (HSO) - (Enter Employee's Name), Organization Code, Room Number, Phone Number, Fax Number, E-mail Address

Alternate HSO(s) - (Enter Employee's Name), Organization Code, Room Number, Phone Number, Fax Number, E-mail Address

HSO Representative(s) - (Enter Employee's Name), Organization Code, Room Number, Phone Number, Fax Number, E-mail Address

Operations Security (OPSEC) Representative - (Enter Employee's Name), Organization Code, Room Number, Phone Number, Fax Number, E-mail Address

Alternate OPSEC Representative - (Enter Employee's Name), Organization Code, Room Number, Phone Number, Fax Number, E-mail Address

Technical Surveillance Countermeasures Officer (TSCMO) - (Enter Employee's Name), Organization Code, Room Number, Phone Number, Fax Number, E-mail Address

cc: HSO
Alternate HSO(s)
HSO Representative(s)
OPSEC Representative
Alternate OPSEC Representative
TSCMO
Office of Information Security, AU-42

This page intentionally left blank.