Chapter 8 Revision History as of 03/25/2020:

3/31/2020

- OPSEC heading, 1st paragraph (page 8-1 line 9) Added: Official Use Only (OUO) and Unclassified Controlled Nuclear Information (UCNI).
- OPSEC Appointments (page 8-1 line 9) Added: The head of each element updates the appointment memorandum each time there is a change to their OPSEC Representative. In the absence of a duly appointed OPSEC Representative, the Headquarter Security Officer (HSO) will carry out the duties of the Representative.
- Element OPSEC Representatives (page 8-2 line 13) Added: Conduct OPSEC assessments within their element and brief their management on the results of the assessment.
- OPSEC Assessments (page 8-3 line 8) Added: The OPSEC assessment is conducted by the program element's OPSEC Representative (at intervals not to exceed 36 months for HQ program elements possessing Top Secret and/or Special Access Program information within their facility(s)). Although the OPSEC Representative conducts the OPSEC assessment of their program element, the HQ OPSEC Program Manager may assist with the assessment if requested to do so by the program element OPSEC Representative (refer to DOE O 471.6, *Information Security*, Section 4 f(3), for more on OPSEC Assessments).
- OPSEC Reviews (page 8-3) Added paragraph: OPSEC Reviews – explanation, requirements, and protocols.
- Information on Publicly Posted Websites (page 8-4 line 5) Added: For this reason, each HQ program element shall review information before it is posted on their agency's web site or released to the general public. This review is necessary to ensure that no CI is released unknowingly and without proper authorization.
- Attachment 800-2 (page 6) Added: Sample OPSEC Assessment Report and Checklist

12/5/2019

- Points of contact (page 8-3) Updated to read: "…call (301) 903-7189 or (301) 903-1974."

Chapter 8
Operations Security Program

This chapter covers the Operations Security (OPSEC) Program in place at U.S. Department of Energy (DOE) Headquarters (HQ) to fulfill the requirements of DOE Order 471.6, Section 4.f, *Information Security.*

The goal of the OPSEC Program is to assist HQ program 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 Official Use Only (OUO), Unclassified Controlled Nuclear Information (UCNI), 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 Critical Information List (CIL). The HQ OPSEC Program provides senior managers with information to make sound risk management decisions concerning the protection of CI and ensure that OPSEC techniques and measures are implemented throughout HQ.

HQ Implementation Procedures

<u>HQ OPSEC Program Manager</u>:

The Director, Office of Headquarters Security Operations (AU-40), is responsible for appointing, in writing, a HQ OPSEC Program Manager. The Program Manager oversees the HQ OPSEC program and is the focal point for all OPSEC related issues. The HQ OPSEC Program Manager is responsible for all aspects of the program including:

- Providing OPSEC techniques and measures to program element OPSEC Representatives.

- Assisting HQ elements in identifying their organization’s CI and maintaining their CIL.

- 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 the Annual Security Refresher Briefings) and related meetings, training, and workshops throughout the HQ.

- At the request of the program element OPSEC Representative, assisting in OPSEC assessments/reviews 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 head of each element, or their designee, shall appoint, in writing, an OPSEC Representative. The OPSEC Representative *should* possess a "Q" or "L" clearance. The appointment memorandum is formatted and addressed as described in the *Sample Appointment Memorandum* included in the Forms/Samples subsection below. The head of each element updates the appointment memorandum each time there is a change to their OPSEC Representative. In the absence of a duly appointed OPSEC Representative, the Headquarter Security Officer (HSO) will carry out the duties of the Representative. The Element OPSEC Representative will:

- Assist in the implementation of current and newly developed OPSEC procedures throughout their organization.

- Make certain that employees in their organization are aware of their OPSEC responsibilities.

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

- Internally coordinate and develop the CIL for their organization.

- As is necessary, prioritize and update their organization's CIL and ensure it reflects current assets, threats, operations and other relevant factors. Submit the information to the HQ OPSEC Program Manager as necessary.

- Conduct OPSEC assessments within their element and brief their management on the results of the assessment. See *OPSEC Assessments* below for specifics on these requirements.

- Assist in implementing corrective measures to mitigate vulnerabilities identified during OPSEC assessments. Ensure these measures are implemented in a timely manner.

- 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 Assessment:

OPSEC assessments are conducted to ensure 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 activities. Results must be documented and shared with the program 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, Headquarters Security Officers, security program managers, and senior officials within the element. The OPSEC assessment is conducted by the program element's OPSEC Representative (at intervals not to exceed 36 months for HQ program elements possessing Top Secret and/or Special Access Program information within their boundaries). Although the OPSEC Representative conducts the assessment of their program element, the HQ OPSEC Program Manager may assist with the assessment if requested to do so by the program element OPSEC Representative (refer to DOE O 471.6, *Information Security*, Section 4 f(3), for more on OPSEC assessments).

OPSEC Review:

An OPSEC review is a broad scope review of a specific facility, program, or activity to determine the level of OPSEC support required. The review is a management tool usually conducted by the program element's OPSEC Representative with assistance from the OPSEC Program Manager if requested. However, the OPSEC Program Manager may elect to conduct an OPSEC review if he/she believes it to be necessary to ensure the protection of sensitive information.

In some cases, activities, programs, or facilities may have no sensitive security interests while others may be highly sensitive. Thus, the level of support may range from simply documenting that no further OPSEC support is required to the establishment of a formal OPSEC program. DOE O 471.6, *Information Security*, Section 4 f(3), will be the determining factor.

It is recommended that an OPSEC review 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:

Certain categories of unclassified information are generally recognized as unsuitable for public release. These include, but are not limited to, controlled unclassified information such as Official Use Only (OUO), Unclassified Controlled Nuclear Information, personally identifiable information (PII), protected Cooperative Research and Development Agreements (CRADA), and export control sensitive subjects. For this reason, each HQ program element shall review information before it is posted on their agency's web site or released to the general public. This review is necessary to ensure that no CI is released unknowingly and without proper authorization. The review ensures the information does not place at unacceptable risk to national security, DOE personnel, and or assets, mission effectiveness, or the privacy of individuals. The responsible program element's OPSEC Representative should periodically review published information to confirm appropriateness and continued compliance with DOE directives. Although not suggested, should it become necessary to post CI on a public site, or otherwise make it available to the public, the element should get approval by the OSFSA and the Office of Public Affairs, General Counsel, and/or Office of Classification, as appropriate, prior to releasing this information. For more information on information review and public release of DOE information see DOE O. 471.6, *Information Security*, Section 4 f(3), and the DOE Handbook, OPSEC, June 2019.

Points of Contact

AU-41 is the office of primary responsibility for the Headquarters OPSEC Program. For more information on OPSEC or questions regarding this chapter, call (301) 903-7189 or (301) 903-1974.

Forms/Samples

Sample Appointment Memorandum (see Attachment 800-1)
Sample OPSEC Assessment Report format (see Attachment 800-2)

ATTACHMENT 800-1

Sample Appointment Memorandum

MEMORANDUM FOR KURT RUNGE
DIRECTOR
OFFICE OF PHYSICAL PROTECTION
OFFICE OF ENVIORNMENTAL 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

cc: HSO
Alternate HSO(s)
HSO Representative(s)
OPSEC Representative
Alternate OPSEC Representative
HSO Program Manager (AU-41)

ATTACHMENT 800-2

Sample OPSEC Assessment Report & Checklist

I. ASSESSMENT REPORT

A. Location Date and Purpose

During the period of__________, an OPSEC assessment was conducted by___________, the OPSEC Representative for _______________. The OPSEC assessment identifies the organization's Critical Information (CI) and any vulnerability to this information as a result of the conduct of daily activities. It also provides recommendations, to upper level management, on how to protect this organization's CI.

The OPSEC Representative (hereafter referred to as the assessor) conducted the assessment by utilizing two methods. Under the first method, the assessor attempted to gain access to CI through processes that would be available to someone outside of the organization with building access. It also involved observing patterned behavior and activity of members of the organization to reveal information about its activities and capabilities. The purpose was to reveal what access an unauthorized individual could gain to the program element's workspaces and information. The second method involved the face-to-face review with members of the organization to determine if CI is being adequately protected.

II. RESULTS

A. Internet Search

An OPSEC assessment Internet search was performed of the organization's website and the information available on the Internet.

Results: *List findings*

B. Public Media/Public Releases

An OPSEC assessment search was performed on open source organization's public media and public releases available on the Internet. Provisions for review of information released to the public are/are not in place.

Results: *List findings*

OFFICIAL USE ONLY (when filled in)

C. Trash/Recycle Containers (Dumpster Diving)

The OPSEC assessor looked in the Forrestal/Germantown recycle and trash containers maintained by Office of Management personnel.

Results: *List findings*

D. Office/Workspace Entry and Search

Germantown/Forrestal Building *(identify the facility (s) where the assessment took place)*

Office/Workspace Entry and Search

The OPSEC assessor entered offices/workspaces and copy rooms to determine if CI or other sensitive information was inadequately protected.

Results**:** *List findings*

Recommendations: *List recommendations for each deficient finding and or observation.*

E. Foreign Visits & Assignments (FV&As)

The program office has/does not have a security plan in place for foreign national visitors. The plan is deemed to be/not to be adequate in accordance with established security requirements and Chapter 6, Foreign Interaction, Headquarters Facilities Master Security Plan (HQFMSP). The program office has escort procedures in place and escorts all foreign nationals during visits (*if applicable*).

Results: The OPSEC assessor did not have any FV&A concerns.

F. Critical Information List

The program office maintains a critical information list (CIL) which is current and correct (or, is not current and is not correct). The CIL was reviewed for accuracy during this assessment. Prior to this assessment the last review of the CIL was accomplished on____________. The assessor has determined that the organization's CI is/is not being adequately protected. A random sampling of assigned personnel indicated that employees know/do not know what a CIL is and are familiar/not familiar with means required to protect the organization's CI.

Observations: *List observations*

Recommendations: *List recommendations*

OFFICIAL USE ONLY (when filled in)

CATEGORY	YES	NO	N/A
Program Management			
Has an OPSEC Representative for the Program Element (PE) been appointed, in writing, by the PE director (reference Chapter 8, OPSEC, Headquarters Facilities Master Security Plan (HQFMSP))? - Is the memo current/correct? Has a copy of the memo been provided to AU-41?			
Does the OPSEC Representative have a copy of the current *Threat Statement* on file and are PE personnel aware of the local threat to DOE HQ?			
Has the OPSEC Representative received any formal OPSEC training and/or certification?			
Does the OPSEC Representative regularly attend quarterly HSO meetings (reference "HSO Duties & Responsibilities", HQFMSP)? - Does the OPSEC Representative pass on relevant security information to his/her assigned personnel?			
OPSEC ASSESSMENTS & REVIEWS			
Has an OPSEC Assessment and/or OPSEC Review been conducted of the PE? - When was the last Assessment conducted? - Was the Assessment documented and on file? - When was the last Review conducted? - Was the Review conducted and on file? NOTE: IAW Chapter 8, OPSEC, HQFMSP and DOE O. 471.6, *Information Security*, OPSEC Assessments are required for HQ organizations maintaining Top Secret (TS) materials and Special Access Programs (SAP) at intervals not to exceed 36 months.			

OFFICIAL USE ONLY (when filled in)

CATEGORY	YES	NO	N/A
CRITICAL INFORMATION			
Does the OPSEC Representative maintain a critical information listing (CIL) of their organization's critical information (CI) IAW Chapter 8, OPSEC, HQFMSP and DOE O. 471.6, *Information Security*. - Is the CIL current/correct? - Has a copy of the CIL been provided to AU-41 (NOTE: at a minimum, the CIL is *Official Use Only*)? - Is the CIL reviewed, at a minimum, annually and is the review documented in the PE's Appendix to the HQFMSP?			
Do PE personnel know what information is critical? - Are employees aware of their PE's CIL NOTE: this can, and should, be determined by a random sampling/interview process of assigned personnel.			
COUNTERMEASURES			
Are sensitive documents/information properly disposed of (reference Chapter 5, CMPC, Chapter 8, OPSEC, and Chapter 13, CUI, HQFMSP)? - Is CUI shredded and/or placed in a plain brown paper burn bag and sent to the Classified Central Destruction Facility (CCDF) for disposal? - Are precautions taken to ensure CUI is never placed in a trash can or recycle bin (e.g., dumpster diving, warning sign placed on recycle bins/receptacles, etc.)?			
Is CI displayed in plain view and visible in common areas for all to see, e.g., bulletin boards, desk tops, left unattended on top of printers, copy machines, etc.?			
Is CUI properly protected in unattended work stations/offices and after duty hours (reference Chapter 8, OPSEC, and Chapter 13, CUI, HQFMSP)?			
Are procedures in place for electronically sending/receiving OUO, PII, and UCNI data to ensure this information is protected? - Are procedures for electronically transmitting CUI information documented/in writing?			

CATEGORY	YES	NO	N/A
Do PE personnel know how to report (and who to report to) security concerns and/or security incidents (reference Chapter 11, Incidents of Security Concern)?			
Do all personnel properly display their DOE badge? Do employees question personnel not properly displaying their DOE badge?			
Are procedures in place to review PE/DOE information posted on social media sites and prior to public release to ensure the data does not contain CUI (OUO, PII, UCNI) information (reference Chapter 8, OPSEC, HQFMSP, and DOE O. 471.6, *Information Security*)?			
HOSTING FOREIGN VISITORS & ASSIGNEES			
Are procedures in place to process and host foreign visitors (reference Chapter 6, Foreign Interaction and Chapter 8, OPSEC, HQFMSP)? - Has a FACTS Data Entry Person been appointed, in writing, IAW DOE Order 142.3, Change 1, *Unclassified Foreign Visit and Assignment Program*, and Chapter 6, Attachment 602-6, HQFMSP? - Are FACTS entries made properly and in a timely manner? - Does the host approve all foreign visitors in FACTS? - Are visit memos prepared and sent to the Office of Physical Protection in a timely fashion and IAW Chapter I, Physical Security, Section 107, HQFMSP? - When required (e.g., High-Level Protocol Visit) has a security plan been developed for hosting foreign visitors and is the plan adequate and adhere to the requirements outlined in Chapter 6, Attachment, 602-9, HQFMSP? - Are escorts properly briefed on their escort duties IAW Chapter 6, Attachment 602, HQFMSP (required for LA/VTR access and during security hours)? - Is the escort's briefing recorded in the organization's Appendix to the HQFMSP (listed under the CMPC Training Records section) IAW Chapter 6, page 601-2, HQFMSP?			
Are Indices Checks of foreign visitors/assignees conducted if and when required and IAW Chapter 6, HQFMSP?			