Chapter 8 Revision History as of 09/19/2024:

10/1/2024

- Strengthened the wording for the requirement for the ODFSA to review and approve release of CI information.
- Added: the requirement for all OPSEC representatives to complete the National Training Center (NTC) on-line course, ISC-300DE *OPSEC Overview, within six months of appointment to OPSEC representative duties (pages 8-3 and 8-8).*
- References to Official Use Only (OUO) removed throughout the chapter and replaced with Controlled Unclassified Information (CUI).
- Attached memorandums updated – references to EHSS 41 replaced with EHSS-42.

3/31/2020

- OPSEC heading, first 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.
- OPSEC Assessment Report and Checklist

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 Controlled Unclassified Information (CUI), 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 Responsibilities

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

The Director, Office of Headquarters Security Operations (EHSS-40), is responsible for appointing, 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 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.
- Assisting in OPSEC assessments/reviews at the request of the program element OPSEC Representative 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.

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

- Assigning and documenting 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 shown in the *Sample Appointment Memorandum*. 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 unless authorized by the HQ Officially Designated Federal Security Authority, the Director of the Office of Environment, Health, Safety and Security.

- 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.

- Attend Complete ISC-300DE, *OPSEC Overview.* This on-line course is available on Learning Nucleus and must be completed within 6 months of appointment as an OPSEC representative.

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 activity. 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. If not conducted as part of the annual security survey 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).

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 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 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 must get approval by the OSFSA, with concurrence by the Office of Public Affairs, General Counsel, and the Office of Classification, as appropriate, prior to releasing this information.

Points of Contact

EHSS-42 is the office of primary responsibility for the HQ OPSEC Program. For more information on OPSEC or questions regarding this chapter, call (240) 478-9202 or (301) 903-9990.

Forms/Samples

Sample Appointment Memorandum

OPSEC Assessment Report and Checklist