Operations Security Program Assessment Report & Checklist

I. ASSESSMENT REPORT

A. Location Date and Purpose

Assessment conducted by an Operations Security (OPSEC) Program Representative

Start date: ______________

End date: ______________

OPSEC Program Rep's Name: ____

The OPSEC Program Representative for this Program Element:

____

The OPSEC Program Assessment identifies the organization's Critical Information (CI) and any vulnerability to this information because of the conduct of daily activities. It also provides recommendations, to upper-level management, on how to protect this organization's CI.

The OPSEC Program 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.

Findings / 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.

Findings / Results: *(List findings)*

C. Trash / Recycle Containers (Dumpster Diving)

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

Findings / 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.

Findings / 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 the Headquarters Facilities Master Security Plan (HQFMSP) - Chapter 6, Foreign Interaction. The program office has escort procedures in place and escorts all foreign nationals during visits (*if applicable*).

Results: *(Example: 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 this date: ______________________

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 below.)*

Recommendations: (*List recommendations below.)*

CHECKLIST CATEGORIES:

I. Program Management

A. Has an OPSEC Representative for the Program Element (PE) been appointed, in writing, by the PE director (reference the Headquarters Facilities Master Security Plan (HQFMSP) – Chapter 8, OPSEC Program)?

○ Yes ○ No ○ N/A

1. Is the memo correct?

○ Yes ○ No ○ N/A

2. Has a copy of the memo been provided to the Office of Headquarters Industrial Security Operations (EHSS-42)?

   ○ Yes ○ No ○ N/A

B. Does the OPSEC Representative have a copy of the current Threat Statement on file and are PE personnel aware of the local threat to the U.S. Department of Energy (DOE) Headquarters (HQ)?

○ Yes ○ No ○ N/A

C. Has the OPSEC Representative received any formal OPSEC training and / or certification? As a minimum, has the OPSEC representative completed ISC-300DE, *OPSEC Overview* within six months appointment to OPSEC representative duties?

○ Yes ○ No ○ N/A

D. Does the OPSEC Representative regularly attend monthly HSO meetings (reference Headquarters Facilities Master Security Plan (HQFMSP) – Chapter 17, HSO Program Duties and Responsibilities)?

○ Yes ○ No ○ N/A

E. Does the OPSEC Representative pass on relevant security information to their assigned personnel?

○ Yes ○ No ○ N/A

II. OPSEC ASSESSMENTS & REVIEWS

A. In accordance with the HQFMSP - Chapter 8, OPSEC Program 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. Has an OPSEC Assessment and / or OPSEC Review been conducted of the PE?

○ Yes ○ No ○ N/A

- When was the last Assessment conducted? ____________________
- Was the Assessment documented and on file? ○ Yes ○ No ○ N/A
- When was the last Review conducted? __________________
- Was the Review conducted and on file? ○ Yes ○ No ○ N/A

B. Does the OPSEC Representative maintain a CIL of their organization's CI in accordance with the HQFMSP - Chapter 8, OPSEC Program and DOE O. 471.6, *Information Security*.

- Is the CIL current / correct?

  ○ Yes ○ No ○ N/A

- Has a copy of the CIL been provided to EHSS-41 (NOTE: At a minimum, the CIL is Controlled Unclassified Information (CUI))?

  ○ Yes ○ No ○ N/A

- Is the CIL reviewed, at a minimum, annually; and is the review documented in the PE's Appendix to the HQFMSP?

  ○ Yes ○ No ○ N/A

C. Do PE personnel know what information is critical?
NOTE: This can, and should, be determined by a random sampling interview process of assigned personnel.

○ Yes ○ No ○ N/A

- Are employees aware of their PE's CIL?

  ○ Yes ○ No ○ N/A

III. COUNTERMEASURES

A. Are sensitive documents and information properly disposed of (reference the HQFMSP - Chapter 5, Classified Matter Protection and Control (CMPC), and the HQFMSP - Chapter 8, OPSEC)?

○ Yes ○ No ○ N/A

- Is CUI shredded and/or placed in a plain brown paper burn bag and sent to the Classified Central Destruction Facility (CCDF) for disposal?

  ○ Yes ○ No ○ N/A

- 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 and receptacles, etc.)?

  ○ Yes ○ No ○ N/A

B. Is CI displayed in plain view and visible in common areas for all to see, e.g., bulletin boards, desktops, left unattended on top of printers, copy machines, etc.?

○ Yes ○ No ○ N/A

C. Is CUI properly protected in unattended workstations and offices and after duty hours (reference the HQFMSP - Chapter 8, OPSEC Program)?

○ Yes ○ No ○ N/A

D. Are procedures in place for electronically sending and receiving CUI and UCNI data to ensure this information is protected?

○ Yes ○ No ○ N/A

- Are procedures for electronically transmitting CUI information documented in writing?

○ Yes ○ No ○ N/A

E. Do PE personnel know how to report (and who to report to) security concerns and / or security incidents (reference the HQFMSP - Chapter 11, Incidents of Security Concern)?

○ Yes ○ No ○ N/A

F. Do all personnel properly display their DOE badge?

○ Yes ○ No ○ N/A

G. Do employees question personnel not properly displaying their DOE badge?

○ Yes ○ No ○ N/A

H. Are procedures in place to review PE and DOE information posted on social media sites and prior to public release to ensure the data does not contain CUI and UCNI (reference the HQFMSP - Chapter 8, OPSEC Program and DOE O. 471.6, *Information Security*)?

○ Yes ○ No ○ N/A

IV. HOSTING FOREIGN VISITORS & ASSIGNEES

A. Are procedures in place to process and host foreign visitors (reference the HQFMSP - Chapter 6, Foreign Interaction and the HQFMSP - Chapter 8, OPSEC Program)?

- Has a Foreign Access Central Tracking System (FACTS) Data Entry Person been appointed, in writing, in accordance with DOE Order 142.3A, CHG 2 (LTDCHG), *Unclassified Foreign Visit and Assignment Program*, and the Sample Delegation of Approval Authority Memorandum in the HQFMSP - Chapter 6, Foreign Interaction?

○ Yes ○ No ○ N/A

- Are FACTS entries made properly and in a timely manner?

○ Yes ○ No ○ N/A

- Does the host approve all foreign visitors in FACTS?

  ○ Yes ○ No ○ N/A

- When required has a security plan been developed for hosting foreign visitors and is the plan adequate and adhere to the requirements outlined in the Sample Specific Security Plan in the HQFMSP - Chapter 6, Foreign Interaction?

  ○ Yes ○ No ○ N/A

- Are escorts properly briefed on their escort duties in accordance with the Unclassified Foreign National Visit and Assignment Escort Briefing in the HQFMSP - Chapter 6, Foreign Interaction (required for LA / VTR access and during security hours)?

  ○ Yes ○ No ○ N/A

- Is the escort's briefing recorded in the organization's Appendix to the HQFMSP (listed under the CMPC Training Records section) in accordance with the HQFMSP – Chapter 6, Foreign Interaction, Section 601, page 601 - 2?

  ○ Yes ○ No ○ N/A