

Assessment recommended procedures

The steps listed below have been used at many Department of Defense (DoD) shore based and forward deployed organizations worldwide with consistent, positive results. It is highly recommended that all the steps be read first to gain insight to the entire assessment process prior to its execution. Although no specific or unique training is required to administer and conduct an OPSEC assessment, it is assumed that the organization's OPSEC Officer and working group members have completed basic OPSEC education and understand OPSEC fundamentals. If training is required, OPSEC training sources are referenced at the very end of this document.

Each step should be completed in the order listed.

Steps:

1. Assemble your Working Group to determine an appropriate execution timeline for this assessment. It is recommended the events proceed in the following order to include, but not restricted to:

- A. In-Brief
- B. Threat brief
- C. Observations
- D. Dumpster dives
- E. Conduct OPSEC interviews
- F. Web Risk Assessment (WRA)
- G. Command program review
- H. Assessment wrap-up

A timeline should be prepared for a basic foundation of operations in support of a Plan of Action & Milestones (POA&M) briefing.

2. Present Commanding Officer with an In-Brief prior to the assessment and obtain approval to proceed.

3. Contact command Intelligence department, (i.e. N2, G2, S2, J2 etc.) or Service investigative branch (i.e. NCIS, OSI, CID, etc.) for a threat brief / analysis of local threat intent and capabilities.

4. Assign team leads for designated portions of the assessment (i.e. Trash review, Interviews, Observations, etc.).

5. Begin assessment in accordance with your POA&M (recommend using templates available in this App). Templates can be edited to your organization's specifications. (Example: If security badges are not worn at your organization, remove reference item from template. Add and or remove items as necessary.)

6. Upon completion of the execution phase, and all information has been gathered, it is recommended the working group begin compiling a comprehensive report to present findings to the Commander. It is recommended a short Power Point brief reflecting these findings and recommendations for corrective action are presented to the Commander.

For further OPSEC assistance, please contact the Naval OPSEC Support Team (NOST) at opsec@navy.mil

**Sources for OPSEC training:

IOSS <https://www.iad.gov/ioss/site/customer.cfm>

JOSE <https://intelshare.intelink.sgov.gov/sites/jiowc/divisions/j31/default.aspx>
(SIPR only)

Army https://www.1stiocmd.army.mil/io_portal/Public/Pages/Pulic_main.cfm

Navy <https://www.nioc-norfolk.navy.mil/operations/opsec>

Air Force <https://www.afiwcmil.lackland.af.mil.opsec/index.cfm>