

## Assessment Purpose:

Determine susceptibility to adversary exploitation

Operations Security (OPSEC) is commonly defined as the process of denying adversaries information about friendly capabilities and intentions by identifying, controlling, and protecting indicators associated with planning operations or other activities (“Loose Lips Sink Ships”). Integral to the OPSEC process is the requirement to conduct regular OPSEC Assessments. The Department of Defense Directive (DoDD 5205.02E) Operations Security, dated 20 June 2012, defines an OPSEC Assessment as “An evaluative process, usually conducted annually, of an operation, activity, exercise, or support function to determine the likelihood that critical information can be protected from the adversary’s intelligence.” Additionally, Joint Pub 3-13.3, Operations Security, dated 04 January 2012, describes an OPSEC assessment as “an intensive application of the OPSEC process to an existing operation or activity by a multi-disciplined team of experts. Assessments are essential for identifying requirements for additional OPSEC measures and for making necessary changes in existing OPSEC measures.”

Assessments are conducted only after an organization has identified its Critical Information (CI). Critical information is defined as “Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequence for friendly mission accomplishment (Joint Pub 1-02). The identification of CI is important in that it focuses the OPSEC Assessment on evaluating protection of vital information rather than attempting to protect all classified or sensitive information. The Critical Information template serves as a good reference to generate a CI list for your organization.

OPSEC assessments are different from security evaluations or inspections in that an assessment attempts to reproduce an adversary’s view of the operation or activity being assessed. Independently, a security inspection seeks to determine if an organization is in compliance with the appropriate security directives and regulations. Essentially, OPSEC assessments enable an evaluation of current OPSEC measure effectiveness.

Although OPSEC Assessment findings are not provided to the assessed unit’s higher headquarters, Commanders or OPSEC assessment teams may forward to senior officials generic lessons-learned on a non-attribution basis. Lessons-learned from assessments should be shared with command personnel in order to advance the command’s OPSEC posture and mission effectiveness. Further, leaders and decision makers are shown the resources required to adequately protect against adversary exploitation. Findings should be labeled and handled at appropriate classification level (SECRET or CONFIDENTIAL) depending upon vulnerability results. See your Information Security Manager for guidance.

**OPSEC Assessment bottom line:** OPSEC is emphasized, security is improved, threat awareness raised and mission success rate increased.