EPRM
Enterprise Protection Risk Management

*The **OPSEC Module** is designed with the principles of the OPSEC process in mind -- to systematically identify, control, and protect critical information. Critical information is information about Department of Defense (DoD) activities, capabilities, or limitations that an adversary seeks to gain military, political, economic, or technological advantage. If revealed to an adversary, such information may be used to degrade mission integrity, cause loss of life, or damage friendly resources. The purpose of the OPSEC module is to automate OPSEC assessments and allow senior leaders to receive trend analysis across the enterprise. The module consists of 90 countermeasure questions comprised of several categories, such as communications, critical information, operations, and program management.*

The DoD has moved to a risk-based assessment and analysis approach in accordance with DoD Directive 5200.43 establishing the Defense Security Enterprise (DSE). DoD Directive 5205.02 establishes policy and assigns responsibilities governing the DoD OPSEC program, and incorporates the requirements of National Security Decision Directive Number 298 that apply to the DoD. It is DoD policy that all DoD missions, functions, programs, and activities be protected by an OPSEC program that implements DoD Manual 5205.02
The level of OPSEC to apply is dependent on the threat, vulnerability, and risk to the assigned mission, function, program, or activity, and available resources. OPSEC and other security information operations programs shall be closely coordinated to account for force protection and the security of information and activities. OPSEC Assessments are required to be conducted annually by the end of the fiscal year in accordance with DoD Manual 5205.02.

HII 11/22

The Operations Security (OPSEC) Module

DATA COLLECTION

The assessment is divided into several process steps, described below. The current step will be indicated with a “Click Here” medallion. A green check mark medallion indicates the section is completed, and a grayed-out lock medallion means the section is not available until the current section is completed.

PROFILE ORGANIZATION—
Describes the organization being assessed and who is conducting the assessment

SCOPE ASSESSMENT—
By design, these questions determine the breadth of assessment questions to be completed by the unit/installation (e.g. if a unit does not possess classified information, a “no” answer to this question will eliminate questions regarding classified information from the assessment.

IDENTIFY ASSETS—
17 asset types organized into 16 categories. Select the assets which are applicable to the assessment. This section can be pre-filled if a pre-scored asset template was inherited or the assessment was copied from a previous assessment. Complete any unanswered questions and make necessary adjustments to an asset’s criticality score, as needed, based on known local data.

CHARACTERIZE THREATS—

13 threat scenarios comprised of 4 threat sources and 6 threat methods. Select threats applicable to the assessment. This section can be pre-filled if a pre-scored asset template was inherited or the assessment was copied from a previous assessment. Complete any unanswered questions and make necessary adjustments to a threat’s rating, as needed, based on known local data.

CONDUCT ASSESSMENT—
90 countermeasures questions organized into 16 categories.

RESOURCES

The 2020 OPSEC benchmarks were developed in 2018 by a collaborative working group serving as a technical advisory resource to guide the overall development of the OPSEC module. The working group primarily focused on updating the assessment questions from the previous version and tailoring the questions to present a risk-based perspective. As a result of the working group’s efforts, the overall number of questions was ultimately reduced resulting in a more streamlined assessment, and the assessment report products for Units and Higher Headquarters were refreshed. The working group relied on the following two resources for the development of the OPSEC module.

DoD MANUAL 5205.02 DoD OPERATIONS SECURITY (OPSEC) MANUAL— This publication implements policy and provides procedures for the management of DoD OPSEC programs. This document gives OPSEC program managers guidance in the principles of the OPSEC process focusing on the protection of critical information through the establishment of procedures and the conduct of education and training.

AIR FORCE INSTRUCTION 10-701 OPERATIONS SECURITY (OPSEC)— This publication provides guidance and procedures on operations security throughout the Air Force and implements Air Force Policy Directive 10-7, *Air Force Information Operations*, as well as DoD Directive 5205.02 and DoD Manual 5205.02-M. AF 10-701 is consistent with guidance in DoD Instruction 8560.01 *Communications Security (COMSEC) monitoring and Information Assurance (IA) Readiness Testing and AF Policy Directive 17-1 Information Dominance Governance and Management.*

EPRM
Enterprise Protection Risk Management

Need assistance or want to provide feedback?

Contact EPRM User Support:

EPRMhelp@HII-TSD.com

or

800.754.4204

(0700-1700 EST, M-F)

Additional Resources:

View user guides, videos, & training:

http://eprmhelp.countermeasures.com/

Save Time

CREATE A TEMPLATE — The Templates featured in EPRM allow Template Managers to create a set of pre-loaded answers or values that can be inherited when an Assessor creates a new assessment. The template is a way to provide common answers, or a baseline for multiple organizational assessments. Unlike assessments, not all questions must be addressed and a template can be used for a single focus, like threat characterization.

COPY FROM A PREVIOUS ASSESSMENT — The "copy from" feature allows users to copy answers from an existing assessment into a new assessment. This saves time when conducting a recurring, periodic assessment. The Assessor still has the ability to modify the copied answers if circumstances have changed since the last assessment period, but they do not need to answer all the questions over again.

DUPLICATE AN EXISTING ASSET — Users can create additional assets as long as the type of asset is already in the assessment. For example, if it was necessary to differentiate two types of Secret information, users could create a duplicate Secret information asset and give different names to each. Utilize the Duplicate Asset button to add a copy of the selected asset.

EXPORT/IMPORT CHECKLISTS — Depending on the speed of local SIPRNET connections, an Assessor may benefit from exporting the Countermeasures checklist as a Microsoft Excel document. Once in Excel, the checklist can be completed on the PC or printed to be completed manually. Once the checklist is complete, Assessors utilize the Upload Responses button to import the checklist back into EPRM.

Show Metrics

GENERATE ASSESSMENT REPORT — Once an assessment is completed and locked, click the Reports button in the Assessment Administration window to access hyperlinks for various report documents, analysis spreadsheets, and presentations based on the selected assessment.

GENERATE MULTI-ASSESSMENT REPORT — EPRM provides users with two options for analyzing multiple assessments in aggregate. Click the Advanced Analysis button to enter the Advanced Analysis screen. Scroll down to the bottom of the page and leave a check (✓) mark next to the individual assessments to be included in the analysis. Or, to conduct analysis for all assessments conducted on a particular node, utilize the "Select Nodes for Analysis" button above the Completed Assessments grid. Leave a check (✓) mark next to the node to be compiled. Users must click the "Apply Node Filter" button to apply the node selection. Regardless of which method is chosen, click the "Continue with Selected Assessments" button to run the analysis.

Administration

SHARE AN ASSESSMENT — Users may provide access to an assessment to other users within their objective hierarchy. Users sharing assessments set the level of access to "Read/Write" or "Read Only".

CHANGE ASSESSMENT OWNER — Users may transfer ownership of their assessment to any other user within their objective hierarchy. Once changed, the original owner no longer has any access to the assessment.

ARCHIVE AN ASSESSMENT — If the Started and Completed Assessments list contains more items than desired, users can move assessments to the Archive tab to hold them separate from the Active assessments. The same process works in reverse, if necessary.