Carnegie Mellon University
Software Engineering Institute

# INSIDER THREAT PROGRAM EVALUATION (ITPE) – OVERVIEW

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

---

**Introduction**

Since 2001, the CERT Division of the Software Engineering Institute (SEI), a federally funded research and development center (FFRDC) at Carnegie Mellon University (CMU) has conducted research and gathered data about actual malicious insider acts including IT sabotage, fraud, theft of confidential or proprietary information, espionage, and potential threats to our Nation's critical infrastructures. The CERT Division has also done research on unintentional insider threats.

This research and work have been done by the SEI Insider Risk Team. To date this center has collected, coded, and analyzed more than 1600 cases of malicious insider attacks and unintentional insider actions that cause organizational damage. The team is also builds resources and practices to help organizations build formal insider threat programs (InTPs).

**What is an insider threat?**

*The potential for an individual who has or had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization.*

This can include: *current or former full, part-time, or temporary employees, contractors, or other trusted business partners.*

*Organizational assets can be: people, information, technology, or facilities*

**What is an insider threat program?**

Executive Order 13587 requires federal agencies that operate or access classified computer networks to implement an insider threat detection and prevention program.

Changes to the National Industrial Security Program Operating Manual (NISPOM) require the same of contractors that engage with such federal agencies.


[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

According to these mandates and guidelines such an initiative is a formal program for deterring, detecting, and mitigating insider threat. The program should be cross-organizational, incorporating expertise and resources from "information assurance, human resources, security, counterintelligence, and other relevant functions and resources to identify and counter insider threat".[1]

**What is the ITPE?**

The evaluation, which is based on the National Insider Threat Task Force (NITTF) minimum standards and Federal mandates for insider threat programs, along other sources of best practices developed by the SEI Insider Risk team, enables organizations to gain a better understanding of the state or robustness of their insider threat program (InTP).

The long-term objective of the ITPE is to assist organizations in reducing exposure to damage from potential insider threats. There are four activities that comprise the ITPE Process:

1. Assessment Planning
2. Pre-Assessment
3. Assessment
4. Post-Assessment

The ITPE consists of interviews, observations and demonstrations of work activity, and document reviews to collect relevant data for the evaluation.

**Why is my organization participating?**

Your organization has requested that the SEI conduct an evaluation of the organization's insider threat program.

**Why am I involved?**

Because your roles and/or responsibilities involve some aspect of activities related to prevention, detection, and response to malicious or unintentional

[1] Source: http://ncix.gov/nittf/docs/National_Insider_Threat_Policy.pdf


[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

insider behavior or actions, your management has selected you to participate.

**What am I expected to do?**

You do not need to prepare in advance. The ITPE team will lead you through the relevant questions about capabilities that relate to your organization. You may be asked to participate in an interview or to perform an activity for observation by the ITPE team. If so, we ask that you

- cooperate with the interviewers or observers
- be available to participate when asked or scheduled
- be prepared to discuss your work activities, roles, and responsibilities
- provide copies of documents and work products as appropriate
- demonstrate specific activities or tools as part of an observation if asked

**How will the information be used?**

The information obtained, collected, and reviewed during this evaluation is considered sensitive. Your responses are confidential. Information that you provide will not, in any way, be attributed to you.

The analysis of consolidated document reviews, interviews, and observations are used to arrive at a set of results for this evaluation. A final report is presented to designated organizational stakeholders.

**Is this an official audit or certification?**

No, it is not an audit or certification of any organizational functions, nor is it a compliance assessment.

**Will our organization be scored on this evaluation?**

The ITPE methodology uses thhree workbooks. Each workbook has a set of capabilities related to the workbook topic. Each capability has a set of indicators used to determine if the capability is being met and if met, at what level of robustness. An indicator is marked as being met or not. Based on


[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

the indicators met, a “level” score is provided. The level definitions are seen below.

| Level | Definition |
|---|---|
| **1: Not Performed** | There is a failure of the organization to fully perform this capability. One or more of the Level 2: Core indicators are not being performed. |
| **2: Core** | The organization performs all of the minimal set of practices as required by the NITTF. All of the Level 2 Core indicators are performed. One or more indicators (but not all) at levels 3 and 4 may also be performed. |
| **3: Enhanced** | The organization has additional practices beyond what is required by NITTF to manage insider threats to improve efficiency and functionality. All of the indicators at levels 2 and 3 are performed. Some (but not all) of the indicators at level 4: Robust may also be performed. |
| **4: Robust** | The organization has extensive practices for effective, efficient, and sustained management of insider threats. All of the indicators at levels 2, 3, and 4 are performed. |

Results from the ITPE can provide the organization with business justification for implementing improvements and revising resources. The scores can be used by an organization to identify gaps in practice. The information can also be leveraged by the organization to help prioritize which improvements should be done first (e.g., which are the most critical or have the highest priority).


[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

## Legal Markings

Copyright 2023 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Internal use:* Permission to reproduce this material and to prepare derivative works from this material for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

External use:* This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

* These restrictions do not apply to U.S. government entities.

Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM23-0883

## Contact Us

Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612

**Phone**: 412/268.5800 | 888.201.4479
**Web**: www.sei.cmu.edu
**Email**: info@sei.cmu.edu