Student Guide

Establishing an Insider Threat Program for Your Organization

Lesson 3: Minimum Standards for an Insider Threat Program

Introduction

Objectives

In this lesson, you will learn about the Minimum Standards for implementing an insider threat program.

Minimum Standards

Core Requirements

How do you develop an insider threat program?

The Minimum Standards contain the core requirements you must fulfill. They center on establishing your program's capability to analyze and respond to evidence of a potential insider threat. You must establish your program's ability to gather, integrate, review, assess, and respond to information derived from a variety of sources. You must also establish procedures for insider threat response actions to both clarify and resolve insider threat matters and to ensure that such response actions are centrally managed. Finally, you must develop procedures to document insider threat matters reported to the program and the response actions taken. These procedures must also ensure timely resolution of matters.

You will learn more about these core requirements throughout this course.

Information collection and analysis sources include:

- Counterintelligence
- Security
- Human resources
- Law enforcement
- User activity monitoring

Response procedures include:

- Threat matter clarification
- Central management of response actions

Documentation and resolution procedures include:

- Reported threats and response actions
- Timely resolution of matters

Ensure Program Access to Information

In order for your program to have any effect against the insider threat, information must be shared across your organization. As part of your insider threat program, you must direct all relevant organizational components to securely provide program personnel with the information needed to identify, analyze, and resolve insider threat matters. You must establish procedures for program requests to access sensitive information, such as special access programs. Ensuring such information will be adequately protected will facilitate cooperation by components.

The Minimum Standards also direct you to establish guidelines for reporting information to the program. This will help individuals understand what and how to report.

Finally, as part of establishing an insider threat program, you must ensure timely access to available intelligence and counterintelligence threat-related information.

You will learn more about these requirements later in this course.

Establish User Activity Monitoring Capability

The Minimum Standards require you to develop a user activity monitoring capability for your organization's classified networks. When establishing your organization's user activity monitoring capability, you will need to establish policies and procedures that determine the scope of the effort. Once the agency determines the recommended actions, the agency may need to allow for another agency, such as the Defense Information Systems Agency, or DISA, to provide the monitoring capability. You will need to execute interagency Service Level Agreements, where appropriate.

You will learn more about these requirements later in this course.

Personnel Training

The Minimum Standards require training for both insider threat program personnel and for cleared employees of your organization. The Minimum Standards designate specific areas in which insider threat program personnel must receive training. In addition, all cleared employees must receive training in insider threat awareness and reporting procedures.

You will learn more about these requirements later in this course.

Review Activity

When you establish your organization's insider threat program, which of the following do the Minimum Standards require you to include?

Select all that apply.

- ☐ Ensure access to insider threat-related information
- ☐ Establish analysis and response capabilities
- ☐ Establish user monitoring on classified networks
- ☐ Ensure personnel are trained

Answer Key

Review Activity

When you establish your organization's insider threat program, which of the following do the Minimum Standards require you to include?

Select all that apply.

- ☑ Ensure access to insider threat-related information
- ☑ Establish analysis and response capabilities
- ☑ Establish user monitoring on classified networks
- ☑ Ensure personnel are trained

Per the Minimum Standards, you must include all of these in your organization's insider threat program.