ESTABLISH AN INSIDER THREAT PROGRAM

On October 7, 2011, the President signed Executive Order 13587, "Structural Reforms to Improve Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information." Executive Order (EO) 13587 directs the heads of agencies that operate or access classified computer networks to have responsibility for appropriately sharing and safeguarding classified information.

In November 2012, the White House issued National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs. These minimum standards provide the departments and agencies with the minimum elements necessary to establish effective Insider Threat Programs and safeguard classified information.

Implementation of the National Insider Threat Policy for cleared industry is outlined in paragraph 1-202, DoD 5220.22-M Change 2 of the National Industrial Security Program Operating Manual (NISPOM) with additional guidance provided in Industrial Security Letter (ISL) 2016-XX and the DSS ODAA Process Manual for the Certification and Accreditation of Classified Systems under the NISPOM.

Requirements:

The NISPOM has identified the following requirements to establish an Insider Threat Program:

- **Designate an Insider Threat senior official who is cleared in connection with the facility clearance.**
- **Establish an Insider Threat Program and self-certify the Implementation Plan in writing to DSS.**
- **Establish an Insider Threat Program group (program personnel) from offices across the contractor's facility, based on the organization's size and operations.**
- **Provide Insider Threat training for Insider Threat Program personnel and awareness for cleared employees.**
- **Monitor classified network activity.**
- **Gather, integrate, and provide for reporting of relevant and credible information indicative of a potential or actual insider threat to deter employees from becoming insider threats; detecting insiders who pose a risk to classified information; and mitigating the risk of an insider threat.**
- **Conduct self-inspections of Insider Threat Programs.**

Getting Started:

Establishing your Insider Threat Program involves more than checking off the requirements. The program requires an implementation plan to gather, share, integrate, identify, and report relevant Insider Threat information from offices across the contractor's facility including security, information security, and human resources; this is based on the organization's size and operations. The Senior Official will need to outline the program and identify staff responsible for planning, implementing, and operating each element. It may be helpful to break the process down into Phases.

During the **Evaluation Phase**, you will need to consider whether existing company policies and procedures are in line with the NISPOM or if changes, updates, or additional items are required. During the **Formulation Phase,** you can develop a plan or add to an existing plan for implementing each requirement under your Insider Threat Program. This job aid will assist you with each requirement area. Click each link on the main page for an overview of the requirement, advice for getting started, best practices, and related policy and training resources. During the **Implementation Phase,** your Insider Threat Program will be formally launched and operational.

Note that during the 6 month implementation period, the SMO must self-certify that they have an implementation plan for insider threat. The self-certification must be in writing (i.e. letter, email). The company is not required to submit the full plan during the implementation phase, but simply a certify that the company has a plan in place. This self-certification must come from the SMO at the company or facility and must be via email, letter, or other written form. NOTE: if one plan is certified for the company, each local facility must provide the certification to their assigned ISR. Full written plans must be made available to DSS upon request and will be part of the review during the SVA.

Best Practices:

While the requirements identified in the NISPOM make up the baseline for establishing an Insider Threat Program, you may find it helpful to further break out associated duties and responsibilities. Consider the list of "Core Elements" when planning your program. Also, remember that organizations both large and small have the same minimum requirements**,** but larger companies will likely have more complex processes for implementation.

Insider Threat Programs are designed to mitigate risk and thus fit into your facility's overall risk management practices.

Related Training and Resources:

- **eLearning Course: Establishing an Insider Threat Program for Your Organization CI122.16**
- **Insider Threat Toolkit Tab: Establishing a Program**

http://www.cdse.edu/catalog/insider-threat.html