



## CONDUCT SELF-INSPECTIONS OF THE INSIDER THREAT PROGRAM



[NISPOM](#) paragraph 1-207b addresses requirements for contractors conducting formal self-inspections, which includes the Insider Threat Program.

### Requirements:

- **1-207 b. Contractor Reviews.** Contractors will review their security system on a continuing basis and shall also conduct a formal self-inspection at intervals consistent with risk management principles. Self-inspections will include the following elements:
- The contractor will prepare a formal report describing the self-inspection, its findings, and resolution of issues found. The contractor will retain the formal report for DSS review through the DSS security vulnerability assessments.
- A senior management official at the cleared facility will certify to the CSA, in writing on an annual basis that a self-inspection has been conducted, senior management has been briefed on the results, appropriate corrective action has been taken, and management fully supports the security program at the cleared facility. A copy of the formal report will be forwarded to DSS.
- Self-inspections by contractors will include the review of representative samples of the contractor's derivative classification actions, as applicable.
- These self-inspections will be related to the activity, information, information systems (ISs), and conditions of the overall security program, to include an Insider Threat program; have sufficient scope, depth, and frequency; and management support in execution and remedy.

### Getting Started:

Your facility is already conducting self-inspections and reviewing security systems in accordance with risk management principles. The new requirements indicate that you will add your Insider Threat



Program to the self-inspection program for review. CDSE offers an eLearning course in [NISP Self-Inspection](#) practices and requirements. In addition, you can follow the guidance in the [NISP Self-Inspection Handbook](#). Remember, your Industrial Security Representative is also a great resource and can guide you through the process.

## **Best Practices:**

**Self-inspection provides an opportunity for audit and improvement, not only for the security program, but also for your Insider Threat Program. Consider these best practices:**

- Identify accountabilities.
- Identify staff able to manage the overall process of an integrated self-inspection program.
- Identify self-inspection compliance to requirements.
- Evaluate appropriateness of performance indicators and metrics (metrics drive behavior).
- Plan and select a self-inspection approach.
- The self-inspection objectives should be clearly defined and understood by all involved.
- Validate the effectiveness of Insider Threat Awareness training.
- Evaluate reporting procedures and employee familiarity with requirements.
- Periodically evaluate new solutions to address Insider Threats.
- Remember that “one size does not fit all” and Insider Threat solution vendors may not support the same protocols and standards.
- Consider the usage of technical and behavioral potential Insider Threat risk indicators.
- Identify risks in your program.
- Identify and prioritize required improvements.

## **Related Training and Resources:**

- eLearning Course: [NISP Self-Inspection IS130.06](#)
- [Self-Inspection Handbook for NISP Contractors](#)
- FSO Toolkit Tab: [Self-Inspections/Assessments](#)