NISP Self-Inspection
IS130v5

Student Guide

February 2024

Center for Development of Security Excellence

Table of Contents

Lesson 1: Course Introduction

Course Introduction

Course Information

Welcome to the NISP Self-Inspection course.

Purpose: Provide a thorough understanding of the NISP self-inspection process

Audience: Facility Security Officers at cleared Department of Defense (DOD) contractor facilities participating in the National Industrial Security Program (NISP), other contractor security personnel, Defense Counterintelligence and Security Agency (DCSA) Industrial Security Representatives (IS Reps), and DOD Industrial Security Specialists

Pass/Fail %: 75%

Estimated completion time: 90 minutes

Course Overview

As the Facility Security Officer, or FSO, for your facility, you are responsible for ensuring that, as a member of the National Industrial Security Program, or NISP, your facility's security program effectively fulfills the requirements outlined in the 32 Code of Federal Regulations, or CFR, Part 117,

National Industrial Security Program Operating Manual, or NISPOM.

In order to meet this responsibility, it is imperative that you are aware of the strengths and weaknesses of your security program. One way to verify and validate the effectiveness of your facility's security program is through self-inspections.

In this course, you will learn about the requirements for conducting a self-inspection and how to effectively conduct one, to ensure that your security program is the best it can be.

Course Objectives

Here are the course objectives. Take a moment to review them.

- Identify the legal and regulatory basis for NISP self-inspections
- Identify the purpose of a NISP self-inspection
- Identify the FSO responsibilities for conducting a NISP self-inspection
- Identify the activities involved in preparing for a self-inspection
- Identify the three steps involved in the recommended NISP self-inspection process
- Identify various methods of conducting a NISP self-inspection

- Identify the elements of a self-inspection that pertain to all NISP facilities
- Recognize the additional elements of a NISP self-inspection that may pertain based on a facility's classified involvement
- Identify techniques for interviewing employees as part of a NISP self-inspection

Course Structure

This course is organized into the lessons listed here.

- Course Introduction
- Introduction to NISP Self-Inspections
- Preparing for Your NISP Self-Inspection
- Conducting Your NISP Self-Inspection
- After Your NISP Self-Inspection

Lesson 2: Introduction to NISP Self-Inspections

Introduction

Course Overview

You have recently been appointed as the Facility Security Officer, or FSO, for Performance Basics. Your organization assesses classified government and industry projects that are, or may be in danger of, failing to meet budget and schedule requirements for the Department of Defense, or DOD. The departing FSO, Nancy Wallace, has briefed you regarding Performance Basics' established security procedures and has recommended that you conduct a self-inspection as the new FSO.

Reviewing the security program at your facility sounds like a great place to begin your role as the new FSO. But what exactly is a self-inspection? Why are self-inspections performed? How do you conduct a self-inspection? We will explore the fundamentals of self-inspections and provide answers to these questions.

Objectives

Before you learn how to conduct a self- inspection, it is important to understand why self-inspections are integral to meeting your responsibilities as an FSO.

Here are the lesson objectives. Take a moment to review them.

- Identify the legal and regulatory basis for NISP self-inspections
- Identify the purpose of a NISP self-inspection
- Identify the three steps involved in the recommended NISP self-inspection process

Why Perform NISP Self-Inspections?

Requirements for Self-Inspections

Why perform a self-inspection?

You work at your facility every day, so you should be exposed to all the elements of your security program in action around you, right? Not necessarily.

The National Industrial Security Program, or NISP, was established by Executive Order 12829.

The NISP is a partnership between ***t***he U.S. Government and private industry that helps to ensure that classified information released to industry is properly protected.

Cleared contractors, like your company, agree to meet all NISP requirements as set forth in the

National Industrial Security Program Operating Manual, or NISPOM.

The NISPOM establishes the baseline security procedures and requirements to ensure that safeguards employed by contractors are adequate for the protection of classified information.

One such requirement, outlined in the NISPOM, states that a recurring government security review of all cleared contractor facilities be conducted.

Additionally, when your company signed the DOD Security Agreement, or DD Form 441, it agreed to comply with NISPOM requirements and grant representatives of the government the right to review the procedures, methods, and facilities utilized by your company in complying with the requirements of the NISPOM.

The requirement to perform self-inspections is outlined in the NISPOM, which mandates that contractors review their security program on a continuing basis and shall also conduct a formal self-inspection at least annually and at intervals consistent with risk management principles.

It is also required that contractors prepare and retain a formal written report of their self-inspection for review by the Defense Counterintelligence and Security Agency, or DCSA.

A senior management official must annually certify to DCSA that a formal self-inspection has been conducted, that other Key Management Personnel, or KMPs, have been briefed on results, corrective actions have been taken if necessary, and management fully supports the security program.

> "CSA will conduct recurring oversight reviews of contractors NISP security programs" - NISP
>
> "Contractors will review their security programs on a continuing basis and conduct a formal self-inspection at least annually and at intervals consistent with risk management principles." - NISP
>
> "The SMO at the cleared facility will annually certify to the CSA, in writing, that a self-inspection has been conducted, that other KMP have been briefed on the results of the self-inspection, that appropriate corrective actions have been taken, and that management fully supports the security program at the cleared facility in the manner as described in the certification." - NISP
>
> "Designated representatives of the Government responsible for reviews pertaining to industrial plant security shall have the right to review, at reasonable intervals, the procedures, methods, and facilities utilized by the Contractor" - DD Form 441

Purpose of Self-Inspections

Consider:

You know that performing a self-inspection fulfills the legal requirement created by your company's participation in the NISP, but do you know some of the other benefits of a self-inspection?

While the government review of your facility's security program is a useful evaluation tool, there is no way the government can provide continuous oversight of your security program.

Self-inspections provide insight into your security program, allowing you to verify that your company is in compliance with the requirements of the NISPOM, thereby ensuring the protection of our national security, safety of our citizens, and most importantly, the safety of our service members.

You are required to provide adequate security training to your company's employees at regular intervals as stated in the NISPOM.

Self-inspections provide you with an opportunity to supplement that training with individual interactions during the actual execution of the inspection.

That training will be through interviews, employee participation, FSO demonstration, and employee feedback.

The government has entrusted your company to protect classified information, and your company accepted the responsibility to do so once it signed, the DD 441 security agreement.

A self-inspection is your opportunity to ensure that this information is, in fact, protected, to validate your company's established security procedures, and to ensure a facility clearance is still valid by reviewing required documentation, such as DD Form 254's and contracts.

In principle, you could have the best security procedures in the world, but how do you know those procedures are doing what you intend unless you validate them?

This is your opportunity to test your procedures and enhance or modify them if necessary. When your government review is conducted, you can be confident about your security procedures and respond with certainty about your self-inspection.

Don't be afraid to share any concerns you may have with your Industrial Security Representative or IS Rep. Sharing your concerns is encouraged so he or she may be able to assist you with those concerns. Your self-inspection will closely resemble a government review. Let's take a look at what a government review is like.

Government Reviews

Understanding Government Reviews

Remember, your company is subject to government reviews according to the NISPOM.

A government security review is performed by a government representative assigned to your facility by your cognizant security agency, or CSA.

For the Department of Defense, or DOD, Department of Homeland Security or DHS, and any of the other user agencies represented by the DOD in the NISP, The Defense Counterintelligence Security Agency, or DCSA, Industrial Security Representative will be the government representative.

Other users of the NISP, such as the Director of National Intelligence, or DNI, Department of Energy, or DOE, and Nuclear Regulatory Commission, or NRC, have their own government representatives.

Government reviews are conducted at intervals consistent with risk management principles and vary depending on your company's classified involvement. These reviews are usually announced in advance.

Government reviews result in the assignment of a security rating. The results of the inspection and the rating assigned to your security program are conveyed to you as the FSO, and your management during the exit briefing of your government review, and again by letter. There are five possible security ratings:

- superior
- commendable
- satisfactory
- marginal
- unsatisfactory

Superior

A rating of superior is reserved for contractors who possess a security posture of the highest caliber when compared with other contractors of similar size and complexity. Such contractors meet the requirements of the NISPOM by consistently and fully implementing procedures that heighten the security awareness of their employees and foster a spirit of cooperation within the security community.

To receive this rating, the contractor must be able to demonstrate the presence of a sustained, high-level of management support. A rating of superior cannot be awarded if any serious security issues were found during the facility's most recent government review.

Commendable

A rating of commendable is assigned to contractors who possess an exemplary security posture when compared with other contractors of similar size and complexity. Such contractors fully implement the requirements of the NISPOM in an effective manner.

The contractor must be able to demonstrate the presence of strong management support for the security program, and there should be no security concerns present that exceed minor administrative issues. A rating of commendable cannot be awarded if any serious security issues were found during the facility's most recent government review.

Satisfactory

The most commonly assigned rating is satisfactory, which denotes that a contractor's security program is in general conformity with the basic requirements of the NISPOM.

This rating may be assigned even if findings requiring corrective action in one or more security program elements resulted from the facility's most recent government review.

Marginal

Contractors are given a rating of Marginal when their security program, for whatever reason, is not in general conformity with the basic requirements of the NISPOM. This rating indicates that serious security issues, with the potential to contribute to an eventual compromise or loss of classified information if left uncorrected, were found during the facility's most recent government review.

When a contractor receives a rating of Marginal, their Government Representative will schedule a follow-up compliance review 120 days after issuing the rating to determine if corrective actions have been implemented.

Unsatisfactory

Contractors are given a rating of Unsatisfactory when circumstances and conditions indicate that the contractor has lost, or is in imminent danger of losing, its ability to adequately safeguard the classified information in its possession or to which it has access. This rating indicates the contractor can no longer credibly demonstrate that it can be depended upon to preclude the unauthorized disclosure of classified information.

When a contractor receives a rating of Unsatisfactory, the Government agencies that have procured services from the contractor are notified of the rating and the circumstances on which it was based, and a compliance security review will be conducted to assess the corrective actions the

contractor is required to implement before their security rating can return to the Satisfactory level.

The Self-Inspection Process

When to Perform NISP Self-Inspections

The departing FSO, Nancy Wallace, recommended that you conduct a self- inspection as the new FSO. Your facility was last inspected four months ago by Veronica Sims, the Industrial Security Representative assigned to your facility.

Consider: Why do you think Ms. Wallace made this recommendation? Are there other times when conducting a self-inspection is appropriate?

You know that you are required to review your security program on a continuing basis and will conduct a formal self-inspection at least annually and at intervals consistent with risk management principles. What does this mean?

It simply means that the assets you are protecting will determine the government review cycle, or the time interval that your IS Rep uses to determine the scope and frequency of your security reviews.

It is recommended that self-inspections be conducted when there are changes to your facility such as the appointment of a new FSO or the award of a new classified contract that contains new or additional security requirements, when there are changes in your company involving ownership, growth and expansion, or relocation, or when problems are found with the current security program.

Risk Management Principles

The purpose of risk management is to provide a systematic approach to acquiring and analyzing the information necessary for protecting assets and allocating security resources.

For more information on risk management, please see the Risk Management for DOD Security Programs course from the Center for Development of Security Excellence.

- Assess Asset: Determine the criticality of an asset. Criticality is based on an asset's importance to security and the degree of impact if the asset is damaged or lost.
- Assess Threat: Determine the nature and degree of threat. A threat is defined as the perceived imminence of intended aggression by a capable entity to harm a nation, a government or its instrumentalities.
- Assess Vulnerability: Determine the nature and extent of vulnerability. Vulnerability is defined as a situation or circumstance, which if left unchanged, may result in the degradation, loss of life, or damage to mission-essential resources.
- Assess Risks: Determine the probability that a threat will occur and the degree of impact on operations should a threat occur.
- Determine Countermeasure Options: Identify countermeasure options that can reduce

or mitigate risk. These options should be assessed by comparing the benefit of implementation to the cost of implementation.dcsasi02_07 Recommended Self-Inspection Process

Recommended Self-Inspection Process

Now that you know when and why to perform a self-inspection, you need to know how to perform a self-inspection. In order to be sure your self-inspection is conducted effectively, it is recommended that you view your self-inspection as a three step process rather than an event.

Preparing for a self-inspection includes developing an inspection strategy, making administrative preparations, compiling research materials, determining inspection scope, and selecting an inspection method.

Conducting the actual self-inspection involves reviewing security records, observing the security practices and procedures in place, and interviewing personnel.

During post self-inspection activities, you will compile the results of your inspection, create feedback based on your findings, and develop improvements and solutions for any security issues you may have encountered.

We will examine each of these stages in greater detail in the following lessons of this course.

Review Activity

Review Activity 1

Which of the following statements are true about regulations requiring self-inspections?

Select True or False for each statement, then check the Answer Key at the end of this Student Guide.

1. The NISPOM requires contractors to conduct a formal self-inspection.

☐ True

☐ False

2. The NISPOM states that government security reviews of all cleared contract facilities will be conducted periodically.

☐ True

☐ False

3. The DD Form 441 states that government representatives have the right to review facilities utilized by the contractor.

☐ True

☐ False

4. The NISPOM states that if a facility receives a rating of commendable or better, no self-inspection needs to be performed.

☐ True

☐ False

Review Activity 2

In each of the following scenarios, determine if conducting a self-inspection would be appropriate. For each question, select the best answer; then check the Answer Key at the end of this Student Guide.

1. Your facility is typically reviewed by the government annually. It was last reviewed by your IS Rep in March and received a rating of "Satisfactory." It is now September and your company was just awarded a new classified contract containing additional security requirements. Would it be appropriate to conduct a self-inspection?

- ☐ Yes, self-inspections should be performed every six months.
- ☐ No, facilities that receive a rating of Satisfactory or better on their previous government review do not need to perform self-inspections for any reason before their next annual review.
- ☐ Yes, self-inspections should be performed when there is any growth or change to your company's classified contracts impacting security requirements.

2. You were informed last Friday that one of the projects at your facility where classified work is performed experienced a security violation that disclosed a serious problem with one of your established security procedures. Would it be appropriate to conduct a self-inspection?

- ☐ No, security violations require investigation and reporting procedures but are not cause to conduct a self-inspection.
- ☐ Yes, when your facility's security program appears to be ineffective, conducting a self-inspection can help determine problem areas.
- ☐ No, the program manager is responsible for addressing this situation since it pertains to the project specifically and not the facility in general.

3. Your organization completed a merger three months ago. There are some new managers and an increase in your organization's size. No classified work is directly affected by the merger, and all new employees hold current clearances. Would it be appropriate to conduct a self-inspection?

- ☐ No, a self-inspection is not needed because none of the changes in management personnel directly affect the classified projects at your facility.
- ☐ No, a self-inspection is not required because the new personnel all hold current clearances.
- ☐ Yes, any time an organization experiences significant change in management or growth, performing a self-inspection can help ensure everyone is aware of the facility's security program.

Review Activity 3

For this question, select the best answer; then check the Answer Key at the end of this Student Guide.

1. At which stage in the recommended self-inspection process are the elements compile results, create feedback, and develop improvements addressed?

- ☐ Preparation
- ☐ Conducting
- ☐ Post Inspection

Lesson Conclusion

Summary

You have completed the Introduction to NISP Self-Inspections lesson.

Lesson 3: Preparing for your NISP Self-Inspection

Introduction

Lesson Introduction

Now that you know what a self-inspection is, why you should perform one, and the recommended self-inspection process, it is time to begin planning your own self-inspection.

What are your responsibilities as a Facility Security Officer, or FSO, while conducting a self-inspection?

Who will you need to work with to ensure that your self-inspection is performed successfully?

What activities are involved in preparing for a self-inspection?

Which inspection method is most appropriate to select for your facility?

In this lesson, we will examine how to prepare for a self-inspection and answer each of these questions.

Objectives

Objectives

As you just saw, conducting an effective self-inspection requires a great deal of planning and preparation.

Here are the lesson objectives. Take a moment to review them.

- Identify the FSO responsibilities for conducting the self-inspection
- Identify the activities involved in preparing for a self-inspection
- Identify various methods of conducting a NISP self-inspection
- Identify the elements of a self-inspection that pertain to all NISP facilities
- Recognize the additional elements of a self-inspection that may pertain based on a company's classified involvement

NISP Self-Inspection Roles and Responsibilities

FSO Responsibilities

As the FSO for a cleared facility operating under the National Industrial Security Program, or NISP, the responsibility for conducting self- inspections rests with you.

It is your responsibility to know when the self-inspection should be conducted.

It is your responsibility to coordinate the timing and resources needed for the self-inspection with

senior management and program managers or department heads.

While you may work with, and designate, security team members to assist you in conducting the self-inspection, the responsibility to ensure that the inspection is performed effectively ultimately rests with you, as the FSO.

The self-inspection process does not end when all of your security procedures have been reviewed and all employee interviews have been completed.

Once the self-inspection is completed, you have the important responsibility of analyzing any findings and determining when and how to revise your facility's security program accordingly.

You must also prepare a formal report describing your self-inspection, its findings, and resolution of any issues found.

This report must be retained for CSA review until your next CSA review occurs.

Finally, contact your DCSA Industrial Security Representative for any advice and assistance.

Now that you understand your responsibilities for conducting a self-inspection, let's examine the roles others may play in supporting you as you conduct your self-inspection.

Roles of Other Participants

NISP self-inspections cannot be successfully performed without the participation and cooperation of key individuals within your company. You will need to gain the support of your facility's senior management. Management's support of your self-inspection demonstrates their commitment to their security program and is instrumental in gaining the cooperation of all employees.

Preparing for, conducting, and responding to self-inspections requires resources that must be allocated by management. A senior management official at your company must also certify to the CSA, in writing and on an annual basis, that your self-inspection was conducted, that your senior management supports your security program and was briefed on the results, and that any appropriate corrective action was taken.

Despite your best efforts, conducting a self- inspection is going to disrupt the normal work processes of your company's employees. One way to minimize this disruption is by coordinating with the project's program manager and making employees aware of the self- inspection, and how they may become involved in that process to include being interviewed, submitting documentation, and demonstrating security procedures, ahead of time.

Developing an Inspection Strategy

What is a Self- Inspection Strategy?

You should model your self-inspection on the government security review.

A guide to assist you in conducting your self-inspection, the Self-Inspection Handbook for NISP Contractors, is available for your use. The Self-Inspection Handbook addresses basic NISPOM requirements through a series of questions arranged according to Elements of Inspection.

Before beginning your self-inspection, it is recommended that you review the Elements of Inspection to determine those that apply to your facility's involvement in the NISP. Once you have your elements identified, you are ready to customize a self-inspection checklist unique to your established security program. Additionally, you should develop an inspection strategy, to outline how you plan to execute your self-inspection. It is actually your self-inspection strategy, not the Self-Inspection Handbook that should direct the sequence and scope of your self-inspection.

You will also find there are certain administrative duties and pre-inspection research that you will have to include in your self-inspection strategy. We will examine each of these self-inspection strategy activities more closely.

Administrative Tasks

There are three administrative tasks that you will need to accomplish when preparing for your self-inspection: securing management support, selecting dates, and notifying your employees of the upcoming self-inspection.

Secure Management Support

As was previously mentioned, securing management support and approval is essential to a successful inspection. When approaching management about demonstrating support for your self-inspection, it may help you to remind them of the benefits a self-inspection provides to your company.

Self-inspections help ensure the protection of classified material and information entrusted to your company. Your facility is required to conduct such inspections. Self-inspections ensure that your facility meets its contractual requirements such as those outlined in the Department of Defense Contract Security Classification Specification, or DD Form 254.

Self-inspections are a way to assess the security posture of your facility and the health of the security program. Evaluating results and making changes, corrections, or improvements will help

your facility prepare for government reviews.

Select Dates

You know it is required that you perform a self-inspection at least annually and at intervals consistent with risk management principles. You, therefore, have a great deal of advance notice about when you should conduct your self-inspection.

When determining the actual date or dates of the self-inspection, be sure to consider: Management and employee availability, contract deliverable schedules and the effort needed to support them, and the duration of the inspection. Select dates that are as accommodating as possible when factoring in each of these considerations.

Notify Employees

An announcement should be made to all personnel advising them of the self-inspection and requesting their cooperation. If possible, have management issue the announcement regarding the inspection. This will serve to make management support of the inspection clear to all personnel, and indicate that management values the self-inspection as an integral element of the facility's security program. Coordination with program managers or department heads is important to ensure a successful inspection with minimal impact on project work.

Make certain that all personnel involved in the inspection are aware of their responsibilities and what may be asked of them.

Inspection Announcement:

Good morning,

In accordance with the requirements outlined by the NISPOM, our security team will be conducting a self-inspection of our facility from July 20 through July 22. All employees are expected to provide full cooperation with members of the security team in their effort to conduct this inspection. Self-inspections are an integral part of this facility's security program and serve to ensure our program is as effective as possible. Our FSO will be coordinating with Program Managers and Department Heads to ensure that project work is minimally impacted by the inspection. All project personnel, both supervisory and subordinate staff, may be subject to requests from our security team to provide required documentation. In addition, all project personnel should be honest and cooperative in employee interviews, and demonstrate our processes and procedures in a manner representative of how normal operations are conducted at this facility. Your assistance in this

effort is appreciated.

Regards,

The Management Team

Performance Basics

Pre-Inspection Research

Consider:

What are some of the pieces of information you might need to know in order to plan a self-inspection? Who might you need to speak with to assess the processes and procedures involved in your company's security program? What topics should you be sure to discuss with each individual?

Answering each of these questions is part of performing pre-inspection research. The NISP Self-Inspection Handbook outlines eight areas for pre-inspection research. First, identify all the security elements that apply to your organization. It is also recommended that you familiarize yourself with your company's business structure and organization.

In addition, determine what records will need review and what personnel you will need to speak with.

Before you begin researching and locating documentation, it is recommended that you create a list of documents that you will need to review and where you can locate them or who might be able to provide them.

Examples of documents you should review include:

- Results of last DCSA security review
- Request for Information
- Current DD Form 254s, properly marked source documents associated with a contract, and classification guides
- Company press releases, publications, and website
- Security records
- Personnel clearance records for cleared employees from the DOD personnel security system of record.

Employee interviews are the best way to determine if the personnel at your facility understand their role and responsibilities in ensuring the protection of classified information. To ensure you cover all facets of the employee's involvement with classified information, you should create a list of individuals who either work on classified projects, or directly oversee the performance on these projects.

Create a list of questions and topics you want to discuss with each individual. This will ensure your interview will remain focused on the inspection. Also consider scheduling meetings in advance to allow personnel adequate time to prepare.

Additional areas of pre-inspection research include becoming familiar with the physical layout of your facility, such as where classified material is stored and where classified work is conducted. It is also important to identify any current threats to your company's technologies, as well as to have a basic understanding of the classified programs at your company. Documents

Pre-Inspection Research - Identify:

1. Applicable security elements
2. Business structure and organization
3. Documents to review and people to interview
4. Questions and topics to cover
5. Physical layout
6. Current threats to technologies
7. Classified Programs

Determining Scope

Part of creating your inspection strategy is determining the scope of what your self- inspection should cover. You will need to tailor your self-inspection to cover the security elements applicable to your facility's classified involvement. To do this, you will need to review the elements outlined in the Self-Inspection Handbook and determine which ones apply to your facility.

The Self-Inspection Handbook is intended to act as a guide to assist you in your self-inspection. You should be careful not to use the handbook as a simple checklist, but as a living document. The best way to use the handbook is to review the security elements and related questions and identify those that apply to your facility's classified operations.

Once you know which questions apply, ask yourself what logical follow-up questions you will want to ask. Don't just check off yes, no, or not applicable to the questions asked in the handbook. For every question answered, you should verify or validate that answer and record descriptive details in the validation section. Remember conducting a self-inspection requires critical analysis of your security

program; it's not just a simple paper check.

You should actually review established security procedures and any classified material, if available. Also, check appropriate security records and interview employees to verify that the information is accurate and current. Rather than just assume that a security policy or procedure is being correctly implemented, you should not only interview your employees you should have them demonstrate how they implement that procedure.

Communicate with your cleared employees on a regular basis. As the individuals who actually implement your security policies and procedures, you can maintain a better awareness of your security program through them.

Applicable Inspection Elements

Consider:

Each facility is unique.

Depending on the level of involvement your facility has in dealing with classified information,

your inspection may have a limited scope or it may need to be a more comprehensive examination.

How would you determine the scope of your inspection?

The Self-Inspection Handbook includes eight elements that apply to all facilities as well as thirteen additional elements that are applicable only to possessing facilities. The eight basic inspection elements that every facility must include in its self-inspection are listed in the Self-Inspection Handbook.

Elements that apply to **all** facilities:

- (117.7) Procedures
- (117.8) Reporting Requirements
- (117.9) Entity Eligibility Determination for Access
- (117.10) Contractor Eligibility for Access to Classified
- (117.11) Foreign Ownership, Control, or Influence (FOCI)
- (117.12) Security Training and Briefings
- (117.3) Classification
- (117.16) Visits and Meetings

Possessing facilities, or those facilities where classified information is received, stored, and possibly

generated, include thirteen additional safeguarding elements. These thirteen elements commonly apply to possessing facilities. They are listed in the Self-Inspection Handbook.

The 13 safeguarding elements common to possessing facilities:

- (117.14) Marking Requirements
- (117.15-a) General Safeguarding
- (117.15-b) Standards for Security Equipment
- (117.15-c) Storage
- (117.15-d) Intrusion Detection System (IDS)
- (117.15-e) Information Controls
- (117.15-f) Transmission of Classified Information
- (117.15-g) Destruction
- (117.15-h) Disclosure
- (117.15-i) Disposition
- (117.15-j) Retention
- (117.15-k) Termination of Security Agreement
- (117.15-l) Safeguarding CUI

This list is not all-inclusive. In special cases, additional elements may apply and should be included in your self-inspection if they relate to your security program. Also, your facility may have a greater degree of classified involvement and additional elements may, therefore, need to be included in your self-inspection.

Because Performance Basics holds a Secret facility clearance with Secret storage and possesses classified information up to the Secret level, the inspection elements that apply include: the eight basic elements common to all NISP facilities and the thirteen safeguarding elements common to most possessing NISP facilities.

Inspection Methods

Selecting an Inspection Method

Consider:

How would you structure your self-inspection to be sure you accurately assess your company's security program?

In order to answer this question, there are some key pieces of information you need to know about your facility and the classified work it performs.

Your organization, Performance Basics, is considered a moderately-sized company. The project portfolio for Performance Basics includes private sector and government projects, some of which require the handling of classified information and materials.

Many of your company's classified projects require personnel to work at the client site, so only a portion of the work performed in your facility is classified. The classified work that is performed in your facility is conducted in an open storage area where classified materials are stored in GSA-approved security containers during non-working hours. The highest level of classified materials stored at your facility is Secret. Finally, the computer system used by your company to conduct classified work is an accredited or authorized system.

Now that you have gathered the relevant information, let's look at how this information will help you determine the best approach to use for your self-inspection. There are two primary inspection methods used to structure a self-inspection: comprehensive and programmatic.

Typically used for smaller facilities, the comprehensive method is based on an examination of the security elements that are applicable to the facility's security program. No particular classified project or program is singled out. A broad view of the security program is taken and from that a determination is made regarding the overall security posture of your company. You can infer from the results of this broad view that the specific programs that support classified contracts have a similar degree of effectiveness in their implementation of the security program.

Typically used for moderate and larger sized facilities, or for more complex facilities, the programmatic approach focuses on a single classified program, project, or contract, and covers all security aspects of that program. You can extrapolate from the results of reviewing this one program and apply these results to the facility's security program as a whole. Because of the size of your facility, and because not every project involves handling classified information, a comprehensive inspection is not practical.

As the FSO, you determine that the programmatic inspection method best fits the needs of your facility and your inspection.

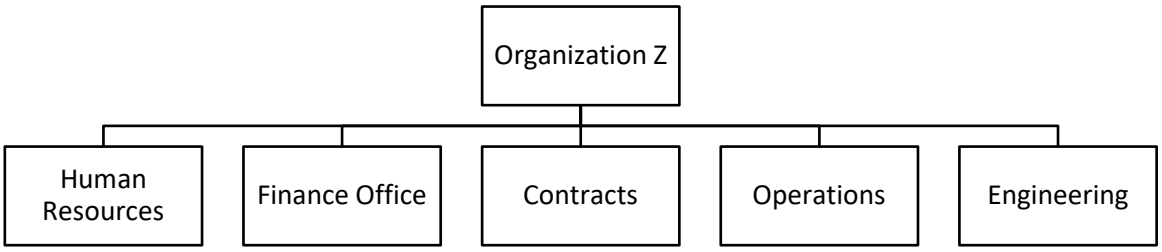
One of the programs that involves handling classified material is called "Axle." You decide to conduct your self-inspection using this program. Read on to learn more about each of the inspection methods.

Comprehensive Inspection Method

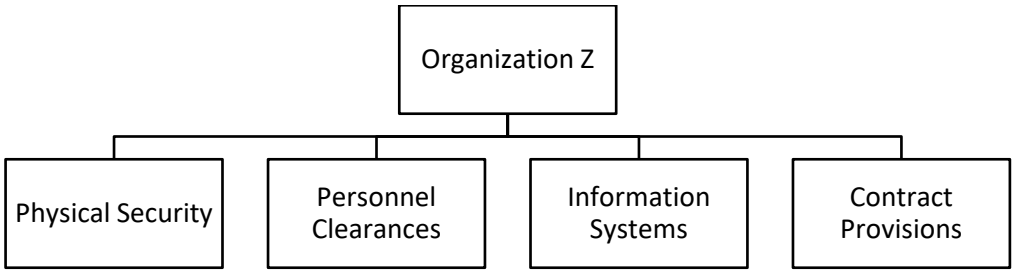
You should note that it is recommended that periodically, all facilities perform a self-inspection

using the comprehensive method. The inspection can be divided up by function or department, or by self-inspection element category.

By Function or Department:



By Inspection Element Category:



Programmatic Inspection Method

Generally, the programmatic inspection method starts with an interview of the program manager to learn what the program is all about. This interview should provide you with a basic overview of the program as well as program details such as level of access, classification procedures, and any problems or problem areas.

Following your interview with the program manager, interview employees working on the program, exploring all security requirements associated with that effort, and conduct a review of any program-related security records.

In larger or more complex facilities, more than one program may be examined. Note that you should not always look at the largest efforts when using this method. Vary the programs selected. Sometimes the smaller efforts need more attention because they are small.

Review Activity

Review Activity 1

Which of the following activities are the responsibility or role of which party?

Select FSO, Management or Program Manager for each statement; then check the Answer Key at the

end of this Student Guide.

1. Recognize when it is appropriate to perform a self-inspection.

- ☐ FSO
- ☐ Management
- ☐ Program Manager

2. Display support for, and allocate resources to, the self-inspection

- ☐ FSO
- ☐ Management
- ☐ Program Manager

3. Arrange appropriate interview times for personnel under his or her purview.

- ☐ FSO
- ☐ Management
- ☐ Program Manager

4. Ensure the self-inspection is conducted effectively and accurately.

- ☐ FSO
- ☐ Management
- ☐ Program Manager

Review Activity 2

Select True or False; then check the Answer Key at the end of this Student Guide.

1. Determining scope is part of preparing for a self-inspection.

- ☐ True
- ☐ False

Review Activity 3

Which of the following inspection elements commonly pertain to which type of facility?

Select "All NISP Facilities" or "Possessing Facilities" for each statement; then check the Answer Key at the end of this Student Guide.

1. Recognize when it is appropriate to perform a self-inspection

- ☐ All NISP Facilities

☐ Possessing Facilities

2. Visits and Meetings

☐ All NISP Facilities

☐ Possessing Facilities

3. Information Controls

☐ All NISP Facilities

☐ Possessing Facilities

4. Contractor Eligibility for Access to Classified

☐ All NISP Facilities

☐ Possessing Facilities

5. Storage

☐ All NISP Facilities

☐ Possessing Facilities

6. Marketing Requirements

☐ All NISP Facilities

☐ Possessing Facilities

7. Security Training and Briefings

☐ All NISP Facilities

☐ Possessing Facilities

Review Activity 4

Given some characteristics about an inspection method, select the inspection method being described.

For each question, select the best answer; then check the Answer Key at the end of this Student Guide.

1. If you examine security elements of a facility's security program and then apply the results of this general examination to specific classified programs, which inspection method are you using?

☐ Comprehensive

☐ Programmatic

2. If you examine only those security elements involved in a particular classified project or program and then apply the results of this specific examination to the company's security program in general, which inspection method are you using?

☐ Comprehensive

☐ Programmatic

Lesson Conclusion

Summary

You have completed the Preparing for Your NISP Self-Inspection lesson.

Lesson 4: Conducting Your NISP Self-Inspection

Introduction

FSO Storyline

You did a great job creating your inspection strategy!

While you were planning for your self-inspection, in addition to the 8 Basic elements that apply to all facilities, you determined which Safeguarding inspection elements will also apply to Performance Basics based on its level of classified involvement and the work performed at the facility. You also determined that the programmatic inspection approach was the most appropriate. Now you are ready to begin your self- inspection.

You will review records, interview employees, observe security processes, and inspect equipment relating to project Axle.

You have met with the Axle program manager, Jared Rogers, to discuss the classified aspects of the project and arrange appropriate times for employee interviews. After your facility's president, Erin Jamison, issued the announcement about your self-inspection, you visited the open storage area for project Axle and met with the employees who work on the project.

You spoke with Jane Larame, a senior business analyst; Christina Herst, a junior business analyst; Stella Lawson, an assistant program manager; Paul Velardi, an engineer; Fiona Johnson, an administrative assistant; and Lester Renard, another administrative assistant.

Before you begin your self-inspection, you decide to take some time to learn more about the activities you will need to perform to conduct your inspection.

Objectives

In order to conduct your self-inspection, you must identify which aspects of your facility's security program you should be examining and what activities are involved in reviewing each aspect.

Here are the lesson objectives. Take a moment to review them.

- Identify the activities involved in conducting a self-inspection
- Identify techniques for interviewing employees as part of a NISP self-inspection

Lesson Overview

Conducting a self-inspection involves three basic activity areas: reviewing security records, interviewing both cleared and uncleared employees, and examining safeguarding systems.

You review security records to verify and validate that your security procedures are effective and are being followed as intended.

You conduct interviews to verify that cleared employees are aware of their security responsibilities and understand the security requirements applicable to their involvement *with classified information at* your facility.

You examine safeguarding systems and equipment**,** and observe safeguarding procedures to verify that classified information is being properly protected to ensure that there has been no unauthorized access to your classified material.

In this lesson, we will discuss these activities in more detail and step through each of them to discover the overall security posture of Performance Basics' security program.

Your Inspection Guide

Recall that in preparing for your self- inspection, you outlined the scope of your inspection by determining which inspection elements apply to your facility.

In the Self-Inspection Handbook, each element includes a comprehensive checklist with a series of questions that address the requirements for that element as laid out in the National Industrial Security Program Operating Manual, or NISPOM. Because each facility is unique, it is possible that not all the questions within each element relate to your security procedures.

Once you have determined which elements apply to your facility's classified activity, you will use the NISPOM in conjunction with the Self-Inspection Handbook to assess your facility's compliance. Each question listed under an inspection element in the Handbook includes a NISPOM paragraph reference. For each question that applies to your facility's classified activities, you should review the associated NISPOM reference and compare it with your established security procedures.

Now, let's look at the Basic inspection elements that apply to all facilities in greater detail.

Self-Inspection Elements

Common to All NISP Facilities

As you learned in the previous lesson, there are eight Basic inspection elements that apply to all cleared contractors, or contractor facilities. Let's examine the intent behind each of these Basic elements.

Basic Elements that Apply to All Facilities:

- (117.7) Procedures
- (117.8) Reporting Requirements
- (117.9) Entity Eligibility Determination for Access to Classified
- (117.10) Contractor Eligibility for Access to Classified
- (117.11) Foreign Ownership, Control, or Influence (FOCI)
- (117.12) Security Training and Briefings
- (117.13) Classification
- (117.16) Visits and Meetings

Procedures

The requirements outlined for the Procedures element will help you to determine if appropriate processes and procedures are in place to protect classified information at your facility.

The following are some key guiding questions to ask as you complete the Procedures section of your Self-Inspection.

- Is there a Standard Practice Procedures in place at your facility?
- Are all appointed security officials adhering to required processes and procedures?
- Are appropriate security measures in place to protect all classified information that the facility is provided access to, or has possession of?
- Has an adequate insider threat program been implemented and maintained per requirements and endorsed by your senior management official, or SMO?
- Has the SMO maintained full accountability for the facility's classified operations?

Keep in mind – this is not intended to be used as just a yes or no checklist when reviewing these general procedures during your self-inspection. A lapse here is an indicator that a facility's security program is lacking in other areas.

Reporting Requirements

This element outlines the Reporting Requirements that help ensure certain events or incidents are reported that could potentially impact your facility's access, or an employee's access to classified information.

When reviewing this element during inspection ask yourself these guiding questions:

- Are cleared employees aware of their reporting responsibilities?
- Are internal procedures established and implemented for cleared employees to report concerning information to the FSO?
- Are employees aware of these procedures?
- Are all reports forwarded as required to the IS Rep, Vetting Risk Operations, or VRO, or the FBI?

During your inspection of this element, reference the Security Executive Agent Directive (SEAD) 3, as needed for any additional guidance.

Entity Eligibility Determination for Access to Classified

Entity Eligibility Determination for Access to Classified, outlines inspection requirements for facilities' that have access to classified information.

- Have there been any changes to any of your Facility Clearance information?
- Are all required forms or records up to date?
- Have the appropriate reports and documentation been executed regarding any changes in key management personnel, or KMPs, FOCI, company name and/or address, ownership, or business structure?

All these factors affect your company's continued capability to maintain its facility clearance to perform on classified contracts.

You should update your facility's information in the FCL System of Record.

Remember, it isn't enough just to answer these questions with a yes or no, you should validate and verify your answer and then record your critical analysis process in the space provided under each applicable element.

Contractor Eligibility for Access to Classified

Contractor Eligibility for Access to Classified is related to making sure the appropriate security procedures are completed in regards to personnel clearances.

- Is the information in the DOD Personnel Security System of Record regarding your cleared employees up to date?
- Have personnel security clearance applications been properly initiated and documented?
- Have individuals with personnel security clearances been given an initial briefing
- and has that clearance been annotated in the DOD Personnel Security System of Record prior to accessing classified information?

Ensuring your personnel clearances are kept to the minimum ensures that only those employees actually working on classified projects have access to classified information.

Foreign Ownership, Control, or Influence (FOCI)

This element applies to all contractors and relates to any material changes affecting the FOCI of your company.

Have any of these changes occurred at your facility?

- Reporting changes in foreign ownership, control and/or influence at your facility to your IS Representative

Have they been promptly reported to your IS Representative using the FCL System of Record?

- Verify changes in FCL System of Record

Major business decisions that could affect your organization's FOCI are often made without the FSO's knowledge. It is important that you stay informed about these decisions because they may affect your facility's continued capability to maintain its security clearance.

Security Training and Briefings

The Element for Security Training and Briefings involves ensuring security training and briefings have been provided to all cleared employees as required. Are the required security records available for verification?

This element also covers if cleared employees are appropriately debriefed when access to classified information is terminated; if training is provided for controlled unclassified information, or CUI, when applicable; and if insider threat awareness training is implemented appropriately.

Keep in mind that knowledgeable employees who are aware of your established security procedures are less likely to violate them. Many times, security violations are the result of a misinformed or uninformed employee.

Appropriate reports submitted for:

- Initial and refresher security training and briefings
- Documenting security training
- Security debriefings
- Controlled Unclassified Information training (CUI)
- Insider threat awareness training

Classification

This element relates to classification guidance as required by the DOD Contract Security Classification Specification, or DD Form 254. The Federal Acquisition Regulation, or FAR, requires that each classified contract must have an accompanying DD 254.

- Has a DD Form 254 been provided for every classified contract issued to your facility?
- Has appropriate classification guidance been forwarded as necessary?
- Is classification guidance adequate to make appropriate derivative classification decisions, if applicable?
- Is all derivatively classified material appropriately marked?
- Are downgrading and declassification actions accomplished as required?

Appropriate classification guidance is essential to ensuring classified materials are handled and protected, appropriately.

- Have the FSO and all derivative classifiers been properly trained?

Visits and Meetings

Visits and Meetings inspection requirements help you to ensure appropriate security procedures are in place to protect classified material during visits, meetings, or seminars.

- Are procedures in place to establish visitors' or attendees' need to know for access to classified information?
- Is each cleared visitor's personnel security clearance being verified?
- Are all cleared visitors properly escorted?

Visitors and attendees of large classified meetings or events pose unique security concerns. Regardless of how familiar a cleared visitor may be to your company or its employees, the requisite security procedures should be applied to every cleared visitor, and every meeting, or seminar, every time.

Common to Possessing NISP Facilities

The eight Basic elements we just examined apply to all NISP facilities; however, because possessing facilities are actually protecting classified material, they must conduct a more extensive inspection.

If your facility has been approved for safeguarding and is storing classified information at your site, then your facility is considered a possessing facility. Because of this responsibility to actually protect classified material, possessing facilities will also need to consider the Safeguarding inspection elements in the scope of a self-inspection. This not an all-inclusive list of the Safeguarding elements common to possessing facilities.

In this lesson, we will review in detail just the Safeguarding self-inspection elements that apply to Performance Basics. Your facility may be subject to additional Safeguarding self-inspection elements depending on its level of actual classified involvement.

Make sure to review the entire list of Safeguarding elements listed in the Self-Inspection Handbook to determine which apply to your facility.

There are 13 Safeguarding elements common to possessing facilities and 5 additional elements that will apply only in special cases. Let's examine the intent behind the Safeguarding self-inspection elements that are unique to Performance Basics.

Marking Requirements

The element for Marking Requirements will help you to verify whether or not classified materials are properly marked during your self-inspection. The purpose of classification markings is to warn and inform the holder that the information is, in fact, classified at a particular level, so they can

implement the appropriate handling and protection requirements.

Appropriate security procedures completed for:

- Accurately marking all classified material
- Applying additional markings as required

Does the classified material received or generated at your facility contain all required markings?

Review the DOD job aid, Marking Classified Information, for additional guidance on marking classified material.

General Safeguarding

General Safeguarding requirements help you to determine whether procedures are in place to protect the classified material stored at your facility. Do cleared employees understand their responsibilities regarding the protection of classified material?

Having policies and procedures in place is important; however, you need to ensure that personnel actually know how to fulfill their responsibilities as cleared employees.

For more information, see the Safeguarding Classified Information in the NISP course.

Standards for Security Equipment

This element covers whether the appropriate security procedures are in place for the storage or protection of classified information at your facility.

Are the established guidelines for security equipment being followed?

- Implementing a system of security measures that ensures classified material is protected in accordance with 32 CFR PART 2001.43 (a)

Is the system of safeguards in place to protect classified materials adequate?

Are the security procedures in place to protect classified material validated and assessed continually and regularly?

- Validating the equipment and security measures in place for protecting classified material

Information Controls

Information controls covers the requirements for:

- An Information Management System (IMS) that protects and controls all classified information

- Top Secret information controls
- Classified working papers
- Combination lock controls
- Information system password controls
- Reproduction of all classified materials

It is required that contractors maintain an IMS to verify and control classified information in their possession. Is there a system in place to track and protect all retained classified information? Does this system include media stored on authorized information systems?

All classified information that your facility has in its possession must be protected and controlled per guidance in the NISPOM. Are controls in place to address accountability, need to know, and, retention of Top Secret information? Are working papers dated, annotated, and destroyed per requirements? Are combinations used to lock secure vaults, open storage areas, and security containers protected in the same manner as the classified information being protected?

Reproducing classified materials should be kept to a minimum and documented appropriately. Is reproduction authorization obtained when required?

Remember that copies of classified information require the same level of protection as originals. Be sure to verify that classification markings were not lost during the reproduction process.

Transmission of Classified Information

Transmission of Classified Information inspection requirements ensures you examine whether the appropriate procedures are in place for the transmission of classified material into and out of your facility, as well as within your facility.

Are required records maintained to confirm this?

- Maintaining required records for Top Secret and Secret material

You are responsible for the protection of classified information during transmission, whether to another facility, or between departments in your own facility.

For more information, see the Transmission and Transportation for Industry Course provided by the Center for Development of Security Excellence.

Disposition

Disposition element requirements help you review whether there are effective processes in place to facilitate the retention, declassification, and/or destruction of classified material at your facility.

Are appropriate records being maintained, when required?

- Documenting the retention, declassification, and/or destruction of classified material

The disposition of classified information comprises many different activities. Your cleared employees should be aware of your established disposition procedures and when and how to document their actions.

Information System Security

The element Information System Security applies only when your organization has authorized information systems used to capture, create, store process or distribute classified information.

The following are some questions you should be asking to determine if security procedures are being followed for these authorized systems.

- Are these systems properly managed to protect against unauthorized disclosure?
  - Ensuring systems are properly managed to protect against unauthorized disclosure of classified information
  - Ensuring policies and procedures are implemented to address, assess, report, isolate, and contain data spills
  - Ensuring policies and procedures are in place to address key components of Insider Threat Program
  - Maintaining continuous awareness of the state of the Information System Security
- Are all policies, procedures, and processes consistent with CSA provided guidance for federal systems?
- Are policies and procedures implemented to address, assess, report, isolate, and contain data spills?
- Is appropriate information system security training provided for authorized users?
- Are processes in place to continuously evaluate threats and vulnerabilities and determine the need for further safeguards?
- Has written authorization for the information system been obtained?
- Do the users understand the need-to-know requirements of the authorized information system?

Many times, employees are simply unaware of the security policies regarding information systems, or they don't realize that their actions constitute a security violation.

Be sure to make your cleared employees aware that all information systems used to process classified information must first be authorized by the CSA. Once the system is authorized, it is the FSO's responsibility to ensure that all system users are aware of the security procedures when using these systems.

Reviewing Security Records

Record Selection

Consider:

You know that you must examine your security records to assist you in assessing your security program's compliance with the NISP, but how would you know which records contain the information you need to review?

As you perform your role as FSO, you will become familiar with the key records and forms related to your security program. If, during your self-inspection, you do not know the specific record or form you need to review to verify one of your security procedures, you should review the NISPOM to see what security records are required, review your facility's standard practice procedures if you have one,

or contact your IS Rep for guidance.

Some of the common security records or forms you may need to review during the course of your self-inspection include your company's DD Form 441, business structure records, KMP list, SF-328 and employees' clearance and briefing records.

Other records, such as those related to your authorized information systems may not apply depending on your organization's level of classified involvement.

Examining Records

Knowing how to effectively verify your security procedures is essential to conducting an accurate and effective self-inspection.

Consider:

With so many responsibilities as an FSO, one sensible way of keeping track of the security procedures in place at your company is maintaining records. Maintaining records also helps you know what you have done, what you need to do, and when you might need to do it again, within your security program. How would you approach trying to review the varied security procedures in place by using security records?

One technique is called sampling. As the name suggests, this technique involves reviewing a sampling of security records related to a specific security procedure as a means of validating that procedure.

Reviewing security records means more than simply making sure that the security record exists.

You must also review the record to assess whether its contents are accurate and complete.

An easy way to verify and validate the records associated with your security procedures is through a simple process called forward and reverse checks. Forward checks begin by reviewing a security record regarding a particular security procedure and then validating the content of the record through interviews and observation.

Reverse checks use the same process as forward checks, only in reverse order. You begin with employee interviews, or observations, and then validate the information gained by reviewing the security records either required by the NISPOM or that you choose to maintain.

Now learn more about examining many of your established security procedures using the sampling technique and learn about verifying your security procedures using the information contained in your security record system.

Sampling

When reviewing your security procedures you may find it helpful to utilize a technique called sampling. Sampling involves validating a security procedure by selecting and reviewing a random sampling of employees and their records within a selected element, for example reviewing Personnel Security Clearance records when inspecting the element Contractor Eligibility for Access to Classified.

Since some records, such as those for Personnel Security Clearances, are used by a wide variety of individuals and programs, this creates a large number of instances of the same security record.

Even if you are conducting a comprehensive self-inspection, it would be unreasonable to review each and every Personnel Security Clearance present in your facility. By reviewing a "sampling" of these security records maintained by your company, you can extrapolate a general status about how effective this security procedure may or may not be.

Forward and Reverse Checks

One technique you may use when verifying your security procedures is called forward and reverse checks. When conducting a forward check, you begin by gathering relevant information concerning a particular security procedure established at your company from your security records. Once you have gathered the relevant information, you verify that information by examining your established security procedures.

Verification activities include observing a classified procedure related to the information, interviewing an employee regarding the information, or examining any associated classified

material that may support the information.

Conducting a reverse check involves implementing the same process, only in the opposite sequence. So, you will instead begin verifying the established security procedure by first either examining classified material, or interviewing or observing an employee, and then you will verify your results from these activities by reviewing the appropriate security records relative to the results.

Security Records Results

Now that you know how to review your security records, let's take a look at the results of the Performance Basics self-inspection.

Review the self-inspection elements to learn what your results are for each one.

Entity Eligibility Determination for Access to Classified

While reviewing security records related to the requirements under Entity Eligibility Determination for Access to Classified, you determined that Performance Basics' Department of Defense Security Agreement, or DD Form 441, and Certificate Pertaining to Foreign Interests, or SF-328, are present, complete, and up to date.

While you believe these records to be complete and up-to-date, it is still a best practice to verify and validate those answers by checking with your senior management, or legal department to ensure what you believe to be true actually is.

Upon reviewing Performance Basics' Key Management Personnel Listing, you found that the recent change to the Board of Directors was not reported.

Contractor Eligibility for Access to Classified

You reviewed personnel clearances as part of your inspection related to element requirements for Contractor Eligibility for Access to Classified, and found that the PCL records for one of your employees, Spencer Richards, indicates he is currently having access despite the fact that the classified project he was working on was completed over four months ago.

Security Training and Briefings

A review of the security training records at Performance Basics revealed that initial security briefings for all newly cleared employees and insider threat awareness training for all cleared employees are up to date. Refresher security training for all cleared employees, however, does not

appear to have been completed. Employee debriefs appear to have been conducted as required.

Classification

A sampling of classified contracts found that a DD Form 254 is present for all classified contracts held at this facility. The program manager provided access to a folder containing all classification guides and any communications requesting additional guidance for project Axle.

Foreign Ownership, Control, or Influence (FOCI)

Security records, confirmed by interviews with senior management, related to requirements under Foreign Ownership, Control, or Influence (FOCI), indicated that the company's SF-328 is complete and accurate, confirming that there have been no changes to report since your last government review.

Employee Interviews

Personnel Categories

Consider:

Who should you interview?

Let's take a look at the different types of personnel that you may need to interview during your self-inspection.

Cleared employees will comprise the majority of the individuals you will want to interview.

Interviewing cleared employees allows you to assess how familiar they are with their security-related responsibilities, and to determine the last time they had access to classified information. Note, however, it is also important not to overlook uncleared employees. The purpose of these uncleared employee interviews is to verify that there has not been any unauthorized access to classified information and to educate them about general security procedures in place.

When conducting a program-specific self- inspection you will always want to start your self-inspection by interviewing the program manager. The purpose of this interview is to learn what the classified program or project is all about.

Other personnel that you should consider interviewing during your self-inspection include any subcontractor employees, long-term visitors, or foreign nationals at your facility to ensure any access to classified information that they may or may not be authorized to have is consistent with the requirements of the NISPOM.

Now view the General Questions that should be asked of a cleared interview candidate.

General Questions

Some questions should usually be asked of every employee.

- What is the level of your clearance and how long have you been cleared?
- When was the last you accessed classified material, at what level, and under what contract?
- When was your last security briefing, what was covered?
- Do you ever use a computer to work on classified information?

Interview Techniques

Conducting a good employee interview can be challenging. Some FSOs have a natural ability to interact well with people, while others may find personnel interviews to be the most difficult aspect of conducting a self-inspection. Regardless of your level of comfort about employee interviews, there are a few techniques you can implement to assist you in making your interviews successful.

- Ask open-ended questions and listen to the responses.
- Allow the interview candidate to respond freely to your open-ended questions.
- Request a demonstration.

Employee interviews are more than in-person quizzes to see if employees know your established security procedures by rote memory. They are your opportunity to determine how classified information is really being handled and protected at your facility and to build relationships with the people in your facility. It is strongly recommended that you foster good working relationships with the employees at your facility, allowing them to feel comfortable coming to you with any security concerns they may have.

Example Conversation:

FSO: “Hi Jane, how are you this afternoon?”

Jane: “Just fine, thanks. How is the inspection going?”

FSO: “I see you have the interview circled on your calendar. I appreciate your willingness to support me in this effort.”

Jane: “We’re a team, you bet!”

Ask Open-Ended Questions

You should phrase your interview questions very carefully. Asking closed-ended questions - questions that can be answered with a simple yes or no response - doesn't allow you to gain any information other than the response to a very specific question. For example, if you asked an individual whether they were involved in a security violation in the past twelve months,

they could respond with a simple "No." You might never learn that although your interview candidate wasn't involved in a security violation, a cleared coworker almost processed classified information on an unauthorized computer system but was stopped by your interview candidate before she actually got started.

Another type of phrasing to avoid is asking leading questions. Leading questions provide the preferred response to the question within the question itself. Read some examples of leading questions and see if you can determine what the question is leading the responder to reply with.

- "Of course, you always conduct your end of day security check before leaving work every day, right?"

  Answer: "Yes I always conduct my end of day security check right before I leave for the day."

- "You didn't use your badge to let your coworker, who forgot his badge, inside the secured area, did you?"

  Answer: "Admitting an individual other than yourself into a secured area using your badge is a security violation; I would never bend the rules, not even for a friend."

- "You would never discuss classified information with someone who didn't have a need to know, would you?"

  Answer: "Discussing a sensitive project with someone who doesn't have a need to know is a violation of our security policy. I would never discuss a sensitive project unless the individual inquiring about the project has a valid need-to-know."

To avoid these problematic phrasings, ask open-ended questions that require more than just a one word response and that do not lead the responder to reply in a particular manner. An example of a good open-ended question is "How do you access classified information on your authorized computer?" This question requires the responder to explain the procedures he or she follows when working on one of the company's authorized information systems, not just reciting the required procedure. From the response, you can determine if the individual is forgetting a key aspect of the security measures related to information systems.

Let people tell their story

An important aspect of a good interview is to be a good listener and to take good notes. Let the interview candidate respond fully before asking any follow-up questions, or moving on to another topic.

When taking notes, always explain the purpose of your notes beforehand, so the person being interviewed isn't caught off guard when you start recording answers to questions being asked. Let them know that the good notes you take, will assist in assessing the results of your self-inspection.

Be flexible! When you ask open-ended questions, you will find that most people feel compelled to reply with a complete story. So be prepared for employees to redirect themselves onto a tangent that is related to the original topic, but which covers far more information than the original response would have provided you.

Allowing employees to tell their story can also lead you to realize that there are more questions you need to ask about a topic – things you may have forgotten, or may not have even thought of, in your list of topics to cover during the interview.

Example Interview:

> Interviewee: "I haven't been involved with any security violations in the last year. I did have to explain about using thumb drives to Lisa, though, when we were making that proposal presentation."
>
> FSO thinks: "Oh, I forgot, I need to ask her about those classified proposal materials."

You may have noticed that most people tend to want to fill in stretches of silence. Leaving a little breathing room between the interview candidate's response and your next inquiry may lead the candidate to fill in the silence with facts, stories, or other information that you might not otherwise have discovered.

Example Interview:

> FSO: "Thank you. I just need to make a few notes."
>
> (silence)

Ask for a Demonstration

Rather than simply asking someone if she is meeting the requirements of the security program when performing work on a classified contract, request a demonstration of the processes and

procedures being used. This accomplishes two things:

- First, you can observe how classified material is actually being handled by the cleared employees at your facility, rather than just knowing that your cleared employees can recite your security procedures when responding to questions;
- And second, it allows for you to form an accurate assessment of your company's security procedures.

By observing your security procedures in action, you may find a more efficient or effective way to accomplish a task.

Practical Exercise: Christina Herst

Apply your understanding of employee interview techniques.

Christina Herst is an analyst working with classified information for project Axle. You need to verify that she understands the requirements regarding classified markings, and that she applies required markings on the classified material she generates on this project.

Select the most appropriately phrased question to ask Ms. Herst in order to achieve your objective.

☐ Option 1: When you generate classified documents for this project, do you apply markings to the documents? Do you place the markings at the top, bottom, front, and back of each page? Do you apply portion markings when there is more than one level of classified information on a page? Do you mark each page with the highest classification level presentment on the page?

☐ Option 2: When you generate classified documents for this project, you place the markings at the top, bottom, front, and back of each page, correct?

☐ Option 3: Could you please demonstrate how you apply classification markings to the classified documents you generate for this project?

Feedback:

☐ Option 1 - Asks Ms. Herst a series of yes or no questions, limiting her replies to only those aspects of the topic that you thought to ask about.

☐ Option 2 - Asks Ms. Herst about implementing classified markings using a leading question, prompting her to reply with the response she knows you would like to hear, rather than with her own knowledge about the topic.

☒ Option 3 - Asks Ms. Herst to demonstrate how she applies classified markings on classified material she generates for this project. This is the most appropriate question as it allows Ms. Herst to demonstrate all that she knows about the topic without prompting her to reply with a particular response.

Results: Christina Herst

Question: "Could you please demonstrate how you apply classified markings to the classified documentation you prepare for this project?"

Answer: "Of course! I always put classification markings on all classified documents I prepare on this project. I stamp "Secret" on the cover page of the document utilizing the markings from the Security Classification Guide."

Ms. Herst responded that she always applies classification markings on any of the classified material she prepares. She marks each document by stamping "Secret" on only the cover page of the document utilizing the markings from the Security Classification Guide.

Ms. Herst appears to be unaware of the need for implementing page and portion markings on the classified material she has generated. This finding should be noted under the self-inspection Element for Marking Requirements.

Practical Exercise: Stella Lawson

Apply your understanding of employee interview techniques.

Stella Lawson is an assistant program manager who coordinates client site operations with work performed at your facility for project Axle. You need to verify that she understands the requirements regarding visitor escorts, and that she implements those requirements appropriately.

Select the most appropriately phrased question to ask Ms. Lawson in order to achieve your objective.

- ☐ Option 1: You are designated as the escort for personnel visiting our facility to assist with project Axle. Could you please demonstrate how such visits normally proceed?
- ☐ Option 2: You are designated as the escort for personnel visiting our facility to assist with project Axle. Do you sign the visitor in? Do you escort the visitor at all times? What other security measures are project personnel expected to implement during a guest visit?
- ☐ Option 3: You are designated as the escort for personnel visiting our facility to assist on this project. You sign the visitor in and escort them at all times, correct? Project personnel implement additional security measures such as obstructing views to classified documents and storing any classified materials not in use, right?

Feedback:

- ☒ Option 1 - Asks Ms. Lawson to explain how she handles a classified visitor at your facility. This is the most appropriate question as it allows Ms. Lawson to explain all that she knows about the topic without prompting her to reply with a particular response.
- ☐ Option 2 - Asks Ms. Lawson a series of yes or no questions, limiting her replies to only those aspects of the topic that you thought to ask about.
- ☐ Option 3 - Asks Ms. Lawson about implementing visitor escort requirements using a leading question, prompting her to reply with the response she knows you would like to hear, rather than with her own knowledge about the topic.

Results: Stella Lawson

Question: "You are designated as the escort for personnel visiting our facility to assist with project Axle. Could you please demonstrate how such visits normally proceed?"

Answer: "Yes, I am the designated escort for this project and have been provided extra training for that designation. I meet visitors downstairs by the receptionist desk, verify their identification, validate their clearance level, and escort them to their point of contact's office for their scheduled visit. Once their visit is complete, I escort them back downstairs to the reception area."

Ms. Lawson responded that she is designated as the escort for this project and has received extra training about her responsibilities. She indicated that she receives visitors and escorts them while they are visiting. Ms. Lawson's response should be noted under the self-inspection Element, Visits and Meetings.

Results: Paul Velardi

Paul Velardi: Administrative Assistant supporting work for project Axle who is responsible for the destruction of any classified material associated with project Axle.

Objective: Verify understanding of requirements regarding the destruction of classified materials.

FSO: "Could you please clarify if this facility has an insider threat awareness program?"

Paul: "Yes, we do have an insider threat program. In fact, we are trained annually on this program's procedures, including how to identify, respond, and report potential threats."

Mr. Velardi's response should be noted under the self-inspection Element Security Training and Briefings.

Results: Fiona Johnson

Fiona Johnson: Administrative Assistant supporting work for project Axle who is responsible for the destruction of any classified material associated with project Axle.

Objective: Verify understanding of requirements regarding the destruction of classified materials and whether those requirements are implemented appropriately when destroying classified documents.

FSO: "Could you please describe what sort of process is followed when classified materials related to project Axle are designated for destruction?"

Fiona: "Oh, yes, when I am notified that SECRET documents needed to be destroyed, I take the material from the security container and put them through the cross-cut shredder designated for classified destruction. Once they are shredded, I check the clippings to make sure that the material was properly shredded."

Ms. Johnson's response should be noted under the self-inspection Element for Disposition.

Safeguarding Systems

Assessing Safeguarding Systems

Consider:

A self-inspection should not only verify a facility's compliance, but also validate the effectiveness of the security measures in place. Part of that is reviewing your safeguarding systems. How would you assess the effectiveness of your safeguarding systems?

Let's take a look at some of the different activities involved in assessing safeguarding systems. There are a few different activities that can help you to assess the effectiveness of your facility's safeguarding systems.

Observing a demonstration of the actual procedures being practiced is one of the best ways to determine if the processes being implemented meet the requirements provided in the NISPOM. For example, you may want to accompany a designated cleared employee as they perform end of day security checks.

Reviewing security violations, if any have occurred since your last inspection, to determine the cause, is a good way to determine whether a safeguarding system may need to be upgraded, replaced, or requires additional training to be used properly.

While your processes can appropriately address security requirements and your facility's personnel can be adequately trained to execute correctly on a well-developed security program, if the mechanical elements involved in securing your facility are faulty, broken, or outdated, your processes and training won't be as effective as they could be.

Take the time to work with operations personnel and conduct an examination of locks, security containers, and intrusion detection systems or IDS.

Safeguarding Systems Results

Let's take a look at the results for your assessment of the safeguarding systems reviewed during your self-inspection.

Read each of the inspection elements to learn what your results are for each one.

Standards for Security Equipment

You examined each of the security containers used for project Axle and determined that all the

security containers were in good order. You validated the procedure followed by the designated cleared employee when performing an end-of-day security check and determined the procedure to be correct.

Transmission of Classified Information

You observed the delivery and receipt of a classified package needed to continue work on this project, from the customer to your facility. The package was received and signed for by a cleared employee, who signed the classified material receipt and returned it to the sender.

The employee maintained direct control over the package, returned to the open storage area for this project, and stored the package in one of the security containers.

Review Activity

Review Activity 1

Select all answers that apply, then check the Answer Key at the end of this Student Guide.

1. What activities are involved with conducting a self-inspection?

- ☐ Employee interviews
- ☐ Review security records
- ☐ Examine safeguarding systems

Review Activity 2

Given a description of a record verification technique, identify which technique is being discussed.

Select the best answer, then check the Answer Key at the end of this Student Guide.

1. Review a security record, then confirm the effectiveness of your established security procedure by conducting employee interviews, observing procedures, and examining physical security components.

- ☐ Sampling
- ☐ Forward Checks
- ☐ Reverse Checks

2. Conduct employee interviews, observe procedures, and examine physical security components, then confirm the effectiveness of your established security procedure by reviewing security

records.

- ☐ Sampling
- ☐ Forward Checks
- ☐ Reverse Checks

Review Activity 3

Given the purpose for using a technique, identify which interview technique is appropriate to use for the given purpose.

Select the best answer, then check the Answer Key at the end of this Student Guide.

1. Because the employee is required to reply with all the information they can recall about the topic, instead of just providing a short answer to a specific question.

- ☐ Ask open-ended questions
- ☐ Let responder tell their story
- ☐ Ask for a demonstration

2. Because you can observe if a step is being overlooked or if a more efficient method has been developed.

- ☐ Ask open-ended questions
- ☐ Let responder tell their story
- ☐ Ask for a demonstration

3. Because the employee may cover more material that is indirectly related to the initial question.

- ☐ Ask open-ended questions
- ☐ Let responder tell their story
- ☐ Ask for a demonstration

Lesson Conclusion

Summary

You have completed the Conducting Your NISP Self-Inspection lesson.

Lesson 5: After Your NISP Self-Inspection

FSO Story Line

Lesson Introduction

That was a lot of work, good job! You completed your review of required documents, conducted personnel interviews with key employees assigned to project Axle, and tested the safeguarding systems in place to protect the classified work performed for this project at your facility.

You have reviewed the elements that comprise your facility's security program. Now you will be able to assess those results and make determinations about what works, what needs improvement, and if there are any holes or gaps in your security procedures.

In this lesson, we will analyze the results of your self-inspection.

Introduction

Objectives

In this lesson, we will learn how to review the results from your self-inspection.

You will learn about post inspection activities such as developing and analyzing your inspection results, providing feedback to your company, and determining what follow-up actions, if any, you should take.

Here is the lesson objective. Take a moment to review it.

- Identify the actions involved in conducting post self-inspection activities

Compiling Self-Inspection Materials

Results

Before you can begin reviewing the results of your inspection, you should compile and organize all the documentation related to the inspection. To facilitate this process and ensure accurate interpretation, you should compile your documentation into the following three categories: Research and Preparation Materials, Self-Inspection Strategy, and Self-Inspection Notes.

Now that your documentation is organized, you can more efficiently develop your inspection results. Here are the results from your self-inspection, organized by each of the inspection elements you reviewed for Performance Basics.

Basic Elements that Apply to All Facilities:

- (117.7) Procedures
- (117.8) Reporting Requirements
- (117.9) Entity Eligibility Determination for Access to Classified
- (117.10) Contractor eligibility for Access to Classified
- (117.11) Foreign Ownership, Control, or Influence (FOCI)
- (117.12) Security Training and Briefings
- (117.13) Classification
- (117.16) Visits and Meetings

Safeguarding Elements that Apply to Performance Basics:

- (117.14) Marking Requirements
- (117.15-a) General Safeguarding
- (117.15-b) Standards for Security Equipment
- (117.15-e) Information Controls
- (117.15- f) Transmission of Classified Information
- (117.15-i) Disposition
- (117.18) Information System Security

Read through these key elements reviewed during your self-inspection to see the results associated with it.

Entity Eligibility Determination for Access to Classified

A review of security records revealed that your DD Form 441 and SF-328 are present, completed, and up to date. The Key Management Personnel List, however, does not appear to be up to date.

Contractor Eligibility for Access to Classified

A review of the personnel security record for Spencer Richards disclosed that his record continues to show current access even though the classified project he was working on was completed over four months ago.

Foreign Ownership, Control, or Influence (FOCI)

A review of documents revealed that the company's SF-328, Certificate Pertaining to Foreign Interests, is present, completed and up to date.

Security Training and Briefings

A review of security records revealed proper security training had been provided to all newly cleared employees. Refresher training for cleared employees, however, has not been conducted.

Additionally, when interviewed, Paul Velardi confirmed that there is an insider threat program at your company and that cleared employees receive annual training which covered procedures for identifying, responding to, and reporting potential threats.

Classification

A review of security records revealed that a DD Form 254, Contract Security Classification Specification, is on file for all classified contracts. Classification guidance is available and is challenged when necessary.

Visits and Meetings

When interviewed, Stella Lawson indicated that she was aware of her responsibilities as the escort for visitors working on a project for Axle or attending a meeting or seminar onsite. She also indicated that she received extra training for her duties as an escort. She indicated that she receives visitors and attendees, verifies their identity and clearance level and escorts them while they are visiting.

Marking Requirements

When interviewed, Christina Herst indicated that she marks each classified document she prepares by stamping “Classified: Secret” on the cover-page of the document. Ms. Herst appears to be unaware of the need for any of the other required markings on the classified material that she generates.

General Safeguarding

You validated the procedure followed by the designated cleared employee when performing an end-of-day security check

and determined the procedure to be correct.

Standards for Security Equipment

You examined each of the security containers used for project Axle and determined that all the security containers are in good order.

Transmission of Classified Information

You observed the delivery and receipt of a classified package from the client to your facility. The package was received and signed for by a cleared employee, who signed the classified material receipt and returned it to the sender. The employee maintained direct control over the package and stored the classified document in one of project Axle's security containers.

Disposition

When interviewed, Fiona Johnson indicated that when she is notified that SECRET documents need to be destroyed she takes the documents and places them in the cross-cut shredder authorized for use with classified material and once the documents have been shredded, she looks through the clippings to make sure the material was properly shredded.

Information System Security

You examined the policies and procedures in place for ensuring systems are appropriately managed to protect against unauthorized disclosure of classified information and project Axle meets requirements. You also observed that effective procedures are in place for maintaining continuous awareness of the state of the Information System Security.

Self-Inspection Results

Self-inspection results comprise more than just your notes. Results consist of your pre-inspection research and preparation materials, your self-inspection strategy, your inspection notes, your findings and your interpretation of them, and any follow-up actions you may implement.

In addition, you must prepare a formal report describing the self-inspection, its findings, and resolution of ***i***ssues found and retain for DCSA to review until after the next DCSA security review is complete.

Developing Self-Inspection Feedback

Feedback

Consider:

Review your notes from your self-inspection of Performance Basics. Are there any individuals, departments, or processes that performed in a remarkable manner?

Feedback should provide relevant facts about the results of your self-inspection. You should indicate positive observations that reflect correctly implemented security practices and procedures, as well as any findings that require correction and the actions necessary to correct those findings.

In addition to these self-inspection highlights, your feedback should provide the overall result of the inspection and a brief explanation about how the result was determined.

"Satisfactory" Rating: Generally conforms to basic NISPOM requirements. Findings requiring corrective action found.

Your feedback should also express thanks to management and employees for their cooperation and assistance in helping you execute the self-inspection.

You can deliver your feedback using several methods:

- Company newsletter
- Company-wide email
- Briefing
- Training sessions

Feedback should be directed to Management and employees at your facility.

When creating your feedback, structure it according to the recommended sequence of topics. Identify any positive observations first, to include any employees who were exceptional in carrying out their security responsibilities, then identify any findings or areas needing improvement. Following that, provide corrective actions for those findings. Continue by indicating the overall inspection result and how it was determined. End your feedback by thanking everyone for their participation.

While your results may reflect many compliant practices, your feedback should highlight those results that reflect outstanding implementation of security measures.

Positive observations:

- Procedures for the handling of incoming classified visitors to the facility
- Transmission procedures for the receipt of classified packages
- Cleared employees aware of your insider threat program and receive annual training

In addition, your feedback should detail those results that require corrective action.

Findings requiring corrective action:

- Facility Clearance documentation not updated with recent change in KMP
- Employee clearances records not updated with current access requirements

- Refresher security training for cleared personnel behind schedule
- Compliant classified markings not implemented consistently

There are four negative findings from your self-inspection of Performance Basics that you will need to correct.

Self-Inspection Feedback

Content:

- Positive observations
- Negative findings and corrective actions for those findings
- Overall inspection results and explanation of how that result was determined
- Express Thanks

Delivery method:

- Company newsletter
- Company-wide email
- Briefing
- Training Sessions

Recipients:

- Management and personnel at facility

Following Up After a Self-Inspection

Follow-Up Activities

Consider:

What would you do to follow up on these findings?

Negative findings:

- Facility Clearance documentation not updated with recent change in KMP
- Employee clearances records not updated with current access requirements
- Refresher security training for cleared personnel behind schedule
- Compliant classified markings not implemented consistently

Once you have determined what the results of your self-inspection indicate about the current state of your facility's security program, you need to conduct follow-up actions in order to ensure that any findings requiring corrective action are appropriately addressed.

Follow-up actions are intended to ensure that corrective actions or improvements have actually been

implemented. Follow-up activities can take many forms.

One of the most frequently used follow-up activities is a visit from you, the FSO, to verify that the recommended practices have been implemented, or that equipment has been repaired or updated.

1. Prepare for Inspection
2. Conduct Inspection – Identify security concerns
3. Post Inspection Activities – Implement resolution and verify effectiveness

Another follow-up activity is creating or correcting a corporate policy document to address a topic absent from existing policy, or unclear in existing policy. You may need to verify that previously non-compliant security records, such as your KMP List and other documents submitted in the DOD Personnel Security System of Record have been updated for completion or accuracy and are now compliant.

Regardless of what other follow-up activities you determine to be appropriate, there is one that you should always perform as the FSO:

You should update your facility's Security Training and Briefings education practices and materials by incorporating the findings and corrective actions from your self-inspection.

Follow-up activities are a very important aspect of self-inspections. Knowing that a security concern exists is the first step to mitigating that issue and implementing the corrective actions necessary to address the concern. This helps ensure that your facility's security program is the best it can be.

To maintain an awareness of how effective your security program has been and what measures you implemented to achieve your current level of effectiveness, you should maintain a record of your solutions, follow-up activities, and the outcomes from your follow-up activities.

IS Rep: "This year's inspection results are an improvement ¬over last year's. How did you effect such a positive result?"

FSO: "We implemented a few updates to our security plan. I can review them with you if you'd like. I'll go get the results from our last self-inspection."

Finally, you must also ensure that a senior management official at your facility will certify to the CSA, in writing, that a self-inspection has been conducted, that senior management has been briefed on the results, that appropriate corrective action has been taken, and that management fully supports the company's security program. This certification must be done on an annual basis.

Consider: What would you do to follow-up on these findings?

- Facility Clearance documentation not updated with recent change in KMP
- Employee clearances records not updated with current access requirements
- Refresher security training for cleared personnel behind schedule
- Compliant classified markings not implemented consistently

Recall that the facility's current KMP List has not been updated to reflect the recent change in Key Management Personnel. Changes to your KMP List can affect your company's continued ability to maintain its facility security clearance, and must therefore be reported immediately.

You decide to have a meeting with the President of the company, Ms. Jamison, to discuss how this kind of information affects your facility's security program and to ensure that you are notified when changes occur in the future.

FSO: "Are you available to meet with me briefly about some security-related concerns I have?"

Ms. Jamison: "Sure. I'm free tomorrow afternoon if that would work."

Remember that you discovered that Spencer Richard's clearance record indicates current access

even though the project he was working on that required the clearance was completed over four months ago.

To address the inconsistency between active personnel security clearances and the projects requiring cleared personnel, you will work with program managers to reconcile active personnel security clearances with the actual number of clearances needed to perform work on classified projects at your facility.

This is a NISPOM requirement and can result in a discrepancy on your security review if not corrected.

As you will recollect, Performance Basics has not provided refresher training to cleared personnel.

To address this issue, you should schedule refresher training to bring the security training schedule up to date and ensure that your facility is compliant with NISPOM requirements.

To address the non-compliant practices regarding classified markings, you should emphasize this aspect in your security training to ensure all employees are aware of the markings required for all classified materials as well as require all individuals doing marking and derivative classifying to complete training pertaining to marking and derivative classification.

FSO Story

Congratulations! You compiled your self-inspection results, created feedback based on the findings, and determined appropriate follow-up activities. You should now be familiar with your facility's security program.

You have recommended to management that an updated security education training program addressing some of the concerns revealed by your self-inspection, to present next month.

You have provided Ms. Jamison with a guide outlining what types of changes to the organization might impact your facility's security clearance, and she has promised to inform you of any changes to the organization that you need to know about as the FSO.

Review Activity

Review Activity 1

Select all that apply; then check the Answer Key at the end of this Student Guide.

1. Self-inspection results comprise which of the following?

- ☐ Pre-inspection research and preparation materials
- ☐ Self-inspection strategy
- ☐ Updated Security Policy
- ☐ Self-inspection findings and the interpretation of those findings
- ☐ Follow-up record
- ☐ Updated security training manual
- ☐ Formal report for DCSA review

Review Activity 2

Select all that apply; then check the Answer Key at the end of this Student Guide.

1. Your feedback should include which of the following?

- ☐ Positive findings
- ☐ Training requirements
- ☐ Negative findings
- ☐ Policy updates
- ☐ Solutions and improvements
- ☐ Express Thanks

2. Which of the following forms of transmission are appropriate to use for your feedback?

- ☐ Newsletter
- ☐ File folder in the security office
- ☐ Email
- ☐ Briefings
- ☐ Training session

3. Recipients of your feedback may include which of the following?

- ☐ Management
- ☐ Program managers
- ☐ Facility personnel
- ☐ Vendors

Review Activity 3

What do you know about follow-up activities?

The purpose of follow-up activities is to ensure that corrective actions or improvements recommended in response to findings have actually been implemented.

Read each statement about follow-up activities and determine if the statement is true or false, then check the Answer Key at the end of this Student Guide.

1. It is true that the purpose of follow-up activities is to ensure that the solutions or improvements recommended in response to negative findings have actually been implemented?

- ☐ True
- ☐ False

2. Follow-up activities can take many forms to include a visit from the FSO, policy update or creation, document verification, and security training.

- ☐ True
- ☐ False

3. You do not need to update your security training by incorporating the findings from your self-inspection.

☐ True

☐ False

4. Senior management is required to certify to the CSA that a self-inspection has been conducted and that appropriate actions have been implemented.

☐ True

☐ False

Lesson Conclusion

Summary

You have completed the After Your NISP Self-Inspection lesson.

Lesson 6: Course Conclusion

Course Conclusion

Course Summary

Conducting self-inspections is a requirement your company agreed to as a cleared contractor operating under the National Industrial Security Program, or NISP. Self-inspections do more than simply fulfill a requirement; they assist you in maintaining an awareness of how your facility's security program is actually being implemented. You should think of performing a self-inspection as a three-step process rather than an event:

1. Preparing for your inspection
2. Conducting your inspection
3. Post-inspection activities

You should now understand how to use the Self-Inspection Handbook for NISP Contractors in conjunction with the 32 CFR Part 117, National Industrial Security Program Operating Manual, or NISPOM, to develop and implement an inspection strategy.

You are now familiar with techniques to assist you in each of the three steps involved in conducting a self-inspection.

Review Security Records

- Sampling
- Forward checks
- Reverse checks

Employee Interviews

- Open-ended questions
- Let respondent tell story
- Demonstration

Safeguarding Systems

- Observe actual procedures in use
- Examine security incidents for root cause
- Examine physical security components

Finally, you should now understand how to use the results of your self-inspection to improve your

facility's security program. Current awareness of your security program's weaknesses and strengths allows you to develop improvements to assist you in protecting the classified information and materials entrusted to your facility, and to you as the Facility Security Officer, or FSO, for your facility.

Lesson Review

Here is a list of the lessons in the course.

- Course Introduction
- Introduction to NISP Self-Inspections
- Preparing for Your NISP Self-Inspection
- Conducting Your NISP Self-Inspection
- After Your NISP Self-Inspection
- Course Conclusion

Course Conclusion

You should now be able to perform all of the listed activities:

- Identify the legal and regulatory basis for NISP self-inspections
- Identify the purpose of a NISP self-inspection
- Identify the FSO responsibilities for conducting the self-inspection
- Identify the three steps involved in the recommended NISP self-inspection process
- Identify various methods of conducting a NISP self-inspection
- Identify the elements of a self-inspection that pertain to all NISP facilities
- Recognize the additional elements of a self-inspection that may pertain based on a company's classified involvement
- Identify techniques for interviewing employees as part of a NISP self-inspection

Congratulations. You have completed the NISP Self-Inspection course.

To receive course credit, you MUST take the NISP Self-Inspection course examination.

Appendix A: Answer Key

Lesson 2 Review Activities

Review Activity 1

1. The NISPOM requires contractors to conduct a formal self-inspection.

☒ True

☐ False

Feedback:

NISPOM states that "Contractors shall…conduct a formal self-inspection…"

2. The NISPOM states that government security reviews of all cleared contract facilities will be conducted periodically.

☒ True

☐ False

Feedback:

NISPOM states that "A periodic security review of all cleared contractor facilities will be conducted…"

3. The DD Form 441 states that government representatives have the right to review facilities utilized by the contractor.

☒ True

☐ False

Feedback:

DD Form 441 - Section II, Security Reviews, states that "Designated representatives of the Government…shall have the right to review, at reasonable intervals, the procedures, methods, and facilities utilized by the Contractor..."

4. The NISPOM states that if a facility receives a rating of commendable or better, no self-inspection needs to be performed.

☐ True

☒ False

Feedback:

Nowhere in the NISPOM does it state that facilities are, for any reason, exempted from the requirement to perform self-inspections.

Review Activity 2

1. Your facility is typically reviewed by the government annually. It was last reviewed by your IS Rep in March and received a rating of "Satisfactory." It is now September and your company was just awarded a new classified contract containing additional security requirements. Would it be appropriate to conduct a self-inspection?

☐ Yes, self-inspections should be performed every six months.

☐ No, facilities that receive a rating of Satisfactory or better on their previous government review do not need to perform self-inspections for any reason before their next annual review.

☒ Yes, self-inspections should be performed when there is any growth or change to your company's classified contracts impacting security requirements.

Feedback:

A self-inspection should be performed since a new classified contract was awarded requiring additional security requirements. Any time there is a significant change to classified contracts, a self-inspection should be performed.

2. You were informed last Friday that one of the projects at your facility where classified work is performed experienced a security violation that disclosed a serious problem with one of your established security procedures. Would it be appropriate to conduct a self-inspection?

☐ No, security violations require investigation and reporting procedures but are not cause to conduct a self-inspection.

☒ Yes, when your facility's security program appears to be ineffective, conducting a self-inspection can help determine problem areas.

☐ No, the program manager is responsible for addressing this situation since it pertains to the project specifically and not the facility in general.

Feedback:

While security violations do require investigation and reporting procedures, and the program manager should be consulted about this incident, it is appropriate to conduct a self- inspection to determine if there are other problem areas.

3. Your organization completed a merger three months ago. There are some new managers and an increase in your organization's size. No classified work is directly affected by the merger, and all new employees hold current clearances. Would it be appropriate to conduct a self-inspection?

☐ No, a self-inspection is not needed because none of the changes in management personnel directly affect the classified projects at your facility.

☐ No, a self-inspection is not required because the new personnel all hold current clearances.

☒ Yes, any time an organization experiences significant change in management or growth, performing a self-inspection can help ensure everyone is aware of the facility's security program

Feedback:

While these changes may not appear to affect your classified projects, it may affect the Foreign Ownership, Control, or Influence criteria of your facility among other security-related elements. Performing a self-inspection will keep you current about your facility's security needs.

Review Activity 3

1. At which stage in the recommended self-inspection process are the elements compile results, create feedback, and develop improvements addressed?

☐ Preparation

☐ Conducting

☒ Post Inspection

Feedback:

Post inspection activities include compiling inspection results, creating feedback, and developing improvements and solutions based on the inspection's findings.

Lesson 3 Review Activities

Review Activity 1

Select FSO, Management or Program Manager for each statement; then check the Answer Key at the end of this Student Guide.

1. Recognize when it is appropriate to perform a self-inspection.

☒ FSO

☐ Management

☐ Program Manager

Feedback:

It is the responsibility of the FSO to recognize when it is appropriate to conduct a self- inspection.

2. Display support for, and allocate resources to, the self-inspection

☐ FSO

☒ Management

☐ Program Manager

Feedback:

Management assists the FSO by demonstrating support for the self-inspection, and by allocating resources for the inspection and the improvement that may result from it.

3. Arrange appropriate interview times for personnel under his or her purview.

☐ FSO

☐ Management

☒ Program Manager

Feedback:

Program managers should coordinate with the FSO to arrange appropriate interview times for project personnel to minimize the impact of the self-inspection on project work.

4. Ensure the self-inspection is conducted effectively and accurately.

☒ FSO

☐ Management

☐ Program Manager

Feedback:

While the FSO may appoint other security team members to assist in performing the self-inspection, and request support from other organization staff, the responsibility of ensuring the inspection is conducted effectively rests solely with the FSO.

Review Activity 2

1. Determining scope is part of preparing for a self-inspection.

☒ True

☐ False

Feedback:

Tailor your self-inspection to cover the security elements applicable to your facility's classified involvement by reviewing the elements outlined in the Self-Inspection Handbook and determining which apply to your facility.

Review Activity 3

Which of the following inspection elements commonly pertain to which type of facility?

Select "All NISP Facilities" or "Possessing Facilities" for each statement.

1. Recognize when it is appropriate to perform a self-inspection

☒ All NISP Facilities

☐ Possessing Facilities

Feedback:

Self-Inspection Element Entity Eligibility Determination for Access, must be included in every NISP facility's self-inspection.

2. Visits and Meetings

☒ All NISP Facilities

☐ Possessing Facilities

Feedback:

Self-Inspection Element, Visits and Meetings, should be included in NISP facilities' self-inspections.

3. Information Controls

☐ All NISP Facilities

☒ Possessing Facilities

Feedback:

Self-Inspection Element Information Controls, should be included in possessing facilities' self-inspections.

4. Contractor Eligibility for Access to Classified

☒ All NISP Facilities

☐ Possessing Facilities

Feedback:

Self-Inspection Element Contractor Eligibility for Access to Classified, must be included in every NISP facility's self-inspection.

5. Storage

☐ All NISP Facilities

☒ Possessing Facilities

Feedback:

Self-Inspection Element Storage, should be included in possessing facilities' self-inspections.

6. Marketing Requirements

☐ All NISP Facilities

☒ Possessing Facilities

Feedback:

Self-Inspection Element Marking Requirements, should be included in possessing facilities' self-inspections.

7. Security Training and Briefings

☒ All NISP Facilities

☐ Possessing Facilities

Feedback:

Self-Inspection Element, Security Training and Briefings, must be included in every NISP facility's self-

inspection.

Review Activity 4

1. If you examine security elements of a facility's security program and then apply the results of this general examination to specific classified programs, which inspection method are you using?

☒ Comprehensive

☐ Programmatic

Feedback:

In the Comprehensive inspection method, you would examine your facility's security program as a whole and then apply the results of that examination to specific classified projects.

2. If you examine only those security elements involved in a particular classified project or program and then apply the results of this specific examination to the company's security program in general, which inspection method are you using?

☐ Comprehensive

☒ Programmatic

Feedback:

In the Programmatic inspection method, you would examine a specific classified program or programs at your facility and then apply the results of that examination to your facility's security program as a whole.

Lesson 4: Review Activities

Review Activity 1

1. What activities are involved with conducting a self-inspection?

☒ Employee interviews

☒ Review security records

☒ Examine safeguarding systems

Feedback:

All answers are correct. Employee interviews include implementing techniques such as asking open-ended questions instead of single-answer or leading questions, allowing the responder to tell their story, and asking for a demonstration.

Document verification includes using the sampling technique to review large quantities of the same document, performing forward checks by reviewing the document and confirming its contents using interviews and observations, and performing reverse checks by conducting interviews or observations first and then confirming their content by reviewing documents.

Validating security measures includes observing a demonstration of actual procedures being implemented, reviewing security incidents to determine the root cause, and conducting an examination of the mechanical elements of your security program.

Review Activity 2

Given a description of a record verification technique, identify which technique is being discussed.

1. Review a security record, then confirm the effectiveness of your established security procedure by conducting employee interviews, observing procedures, and examining physical security components.

☐ Sampling

☒ Forward Checks

☐ Reverse Checks

Feedback:

Forward checks begin with reviewing a security record followed by verifying effectiveness of your

established security procedure through other sources of information such as employee interviews, observing procedures, or examining physical security components.

2. Conduct employee interviews, observe procedures, and examine physical security components, then confirm the effectiveness of your established security procedure by reviewing security records.

☐ Sampling

☐ Forward Checks

☒ Reverse Checks

Feedback:

Reverse checks begin with activities such as employee interviews, observing procedures, or examining physical security components followed by reviewing security records to verify the effectiveness of your established security procedure.

Review Activity 3

Given the purpose for using a technique, identify which interview technique is appropriate to use for the given purpose.

1. Because the employee is required to reply with all the information they can recall about the topic, instead of just providing a short answer to a specific question.

☒ Ask open-ended questions

☐ Let responder tell their story

☐ Ask for a demonstration

Feedback:

Asking open-ended questions avoids limiting the employee's reply to only the information a single-answer question, such as a "yes/no" question, would provide. This technique also avoids prompting the employee to answer in a particular manner to provide the preferred response, such as when asking a leading question.

2. Because you can observe if a step is being overlooked or if a more efficient method has been developed.

☐ Ask open-ended questions

☐ Let responder tell their story

☒ Ask for a demonstration

Feedback:

Your self-inspection should assess what actually takes place at your facility to comply with the requirements of your security program, not whether personnel have memorized security policy.

3. Because the employee may cover more material that is indirectly related to the initial question.

☐ Ask open-ended questions

☒ Let responder tell their story

☐ Ask for a demonstration

Feedback:

You may realize there are more inquiries you need to make about a topic based on the employee's expanded reply. The employee's expanded reply may prompt you to remember topics you forgot you needed to discuss with the interview candidate.

Lesson 5: Review Activities

Review Activity 1

1. Self-inspection results comprise which of the following?

☒ Pre-inspection research and preparation materials

☒ Self-inspection strategy

☐ Updated Security Policy

☒ Self-inspection findings and the interpretation of those findings

☒ Follow-up record

☐ Updated security training manual

☒ Formal report for DCSA review

Feedback:

The correct answers are highlighted. Self-inspection results comprise six elements: pre-inspection materials, inspection strategy, inspection notes, inspection findings and the interpretation of those findings, a follow-up record, and a formal report retained for DCSA review.

Review Activity 2

1. Your feedback should include which of the following?

☒ Positive findings

☐ Training requirements

☒ Negative findings

☐ Policy updates

☒ Solutions and improvements

☒ Express Thanks

Feedback:

Feedback should include positive findings, negative findings, and solutions and improvements.

Training requirements and policy updates should be discussed with the President.

2. Which of the following forms of transmission are appropriate to use for your feedback?

☒ Newsletter

☐ File folder in the security office

☒ Email

☒ Briefings

☒ Training session

Feedback:

Feedback can be provided in the form of a newsletter, email, briefing, or training session and should be accessible to all personnel.

3. Recipients of your feedback may include which of the following?

☒ Management

☒ Program managers

☒ Facility personnel

☐ Vendors

Feedback:

Feedback should be provided to management, program managers, and facility personnel. Vendors do not need to be provided feedback from your self-inspection.

Review Activity 3

Read each statement about follow-up activities and determine if the statement is true or false

1. It is true that the purpose of follow-up activities is to ensure that the solutions or improvements recommended in response to negative findings have actually been implemented?

☒ True

☐ False

Feedback:

It is true that the purpose of follow-up activities is to ensure that the solutions or improvements recommended in response to negative findings have actually been implemented.

2. Follow-up activities can take many forms to include a visit from the FSO, policy update or creation, document verification, and security training.

☒ True

☐ False

Feedback:

It is true that follow-up activities can take many forms to include a visit from the FSO, policy update or creation, document verification, and security training.

3. You do not need to update your security training by incorporating the findings from your self-inspection.

☐ True

☒ False

Feedback:

It is false that you do not need to update your security training by incorporating the findings from your self-inspection. You should always strive to keep your security training current and tailored to your facility's needs.

4. Senior management is required to certify to the CSA that a self-inspection has been conducted and that appropriate actions have been implemented.

☒ True

☐ False

Feedback:

It is true that senior management is required to certify to the CSA (DCSA), annually and in writing, that a self-inspection was conducted, that senior management was briefed on the results, that corrective actions were taken, and that senior management supports the security program.