

# Student Guide

## Course: NISP Self Inspection

### *Lesson 1: Course Introduction*

#### 1. Course Information

<b>Purpose</b>	Provide a thorough understanding of the NISP self inspection process
<b>Audience</b>	Facility Security Officers at cleared Department of Defense (DoD) contractors participating in the National Industrial Security Program, other contractor security personnel, Defense Security Service Industrial Security Representatives, and DoD Industrial Security Specialists
<b>POC</b>	<a href="mailto:IndustrialSecurity.Training@dss.mil">IndustrialSecurity.Training@dss.mil</a>
<b>Pass/Fail %</b>	75%
<b>Estimated completion time</b>	120 minutes

Welcome to the NISP Self Inspection course.

#### 2. 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 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.

#### 3. Course Objectives

Here are the course objectives:

- 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 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 interview techniques for interviewing employees as part of a NISP self inspection

#### **4. 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
- Course Conclusion

# Student Guide

## **Course: NISP Self Inspection**

### ***Lesson 2: Introduction to NISP Self Inspections***

#### **Introduction**

##### **1. FSO Storyline**

*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. 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? In the screens that follow, we will explore the fundamentals of self inspections and provide answers to these questions.*

##### **2. 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:

- 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?**

##### **1. 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 the U.S. Government and private industry 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 DoD 5220.22-M, more commonly called 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 NISPOM 1-206a, states that a periodic government security inspection of all cleared contractor facilities will 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 NISPOM 1-206b, which mandates that contractors review their security program on a continuing basis and shall also conduct a formal self inspection. You can review the NISPOM using the Resource Tool provided on the DSS website: [www.dss.mil](http://www.dss.mil)

“The Contractor agrees to provide and maintain a system of security controls within the organization in accordance with the requirements of the "National Industrial Security Program Operating Manual," DoD 5220.22-M...”  
DD Form 441, Section I – Security Controls (A)

“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 in complying with the requirements of the terms and conditions of the Manual.”  
DD Form 441, Section I – Security Reviews

“**Government Reviews.** Periodic security reviews of all cleared contractor facilities will be conducted to ensure that safeguards employed by contractors are adequate for the protection of classified information.”  
NISPOM 1-206. Security Reviews (a)

“**Contractor Reviews.** Contractors shall review their security system on a continuing basis and shall also conduct a formal self-inspection at intervals consistent with risk management principles.”  
NISPOM 1-206. Security Reviews (b)

## 2. 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 inspection 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 more importantly, the safety of our service members.

You are required to provide adequate security training to your company's employees at regular intervals. Self inspections provide you with an opportunity to supplement that training with individual interactions during the actual execution of the inspection.

The government has entrusted your company to protect classified information, and your company accepted the responsibility to do so once it signed the security agreement. A self inspection is your opportunity to ensure that this information is, in fact, protected and to validate your company's established security procedures. 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 inspection 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 government representative, she may be able to help you address them. Your self inspection will closely resemble a government inspection. Let's take a look at what a government inspection is like.

## **Government Inspections**

### **1. Understanding Government Inspections**

Remember, your company is subject to government inspections according to NISPOM 1-206a. A government security inspection is performed by a government representative assigned to your facility by your government contracting agency. For the Department of Defense, or DoD, and any of the twenty-three user agencies represented by the DoD in the NISP, the Defense Security Service Industrial Security Representative will be the government representative. Other users of the NISP, such as the Central Intelligence Agency, Department of Energy, and Nuclear Regulatory Commission, have their own government representatives.

Government inspections are conducted every 12 or 18 months depending on your company's classified involvement. These inspections are usually announced in advance. Government inspections result in the assignment of a security rating. There are five possible security ratings: superior, commendable, satisfactory, marginal, and unsatisfactory. You may review Industrial Security Letter 2006-02 for more information regarding security ratings.

#### **a. 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 inspection.

#### **b. 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 inspection.

### **c. 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 inspection.

### **d. 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 inspection. 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.

### **e. 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**

### **1. 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 intervals consistent with risk management principles. At a minimum, it is recommended that your self inspection be conducted midway between your government inspections. Government inspections are usually conducted every 12 or 18 months. The frequency of your self inspection depends on the frequency of your government inspection. If your company is inspected every 12 months, your self inspection would be conducted 6 months after your government inspection. If your company is inspected every 18 months, your self inspection would be conducted 9 months after your government inspection.

In addition, 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.

*As you have just learned, there are several circumstances when conducting a self inspection is appropriate. The appointment of a new FSO, such as yourself, is one of those circumstances because performing a self inspection will not only help you to familiarize yourself with your security program, but it will also validate that the established procedures are working. The midway point between government inspections, which is the recommended interval for performing a self inspection, is still two months away.*

#### **a. 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 Center for Development of Security Excellence's Risk Management for DoD Security Programs course.

### **2. 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 completely and accurately, it is recommended that you structure your self inspection process into three stages.

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, interviewing personnel, and observing the security practices and procedures in place. 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 1

Which of the following statements are true about the regulations requiring self inspections? Select True or False for each statement. Check your answers in the Answer Key at the end of this Student Guide.

	True	False
The NISPOM requires contractors to conduct a formal self inspection.	<input type="radio"/>	<input type="radio"/>
The NISPOM states that a government security inspection of all cleared contractor facilities will be conducted periodically.	<input type="radio"/>	<input type="radio"/>
DD Form 441 states that government representatives have the right to review facilities utilized by the contractor.	<input type="radio"/>	<input type="radio"/>
The NISPOM states that if a facility receives a rating of commendable or better, no self inspection needs to be performed.	<input type="radio"/>	<input type="radio"/>

## Review Activity 2

For each question, select the best answer. Check your answers in the Answer Key at the end of this Student Guide.

- 1) Your facility, which is inspected every twelve months, was last inspected by an IS Rep in March and received a rating of "Satisfactory." No other inspections have been conducted since then and it is now December. Would it be appropriate to conduct a self inspection?
  - Yes, self inspections should be performed every three months.
  - No, facilities that receive a rating of Satisfactory or better do not need to perform self inspections.
  - Yes, self inspections should be performed midway between government inspections and it is now three months after the midway point.
- 2) You were informed last Friday that one of the projects on which classified work is performed at your facility 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 incidents 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 his 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

*At which stage in the recommended self inspection process are these elements addressed? Match each stage of the self inspection process to the elements that are addressed in each. Check your answer in the Answer Key at the end of this Student Guide.*

- |                    |   |  |
|--------------------|---|--|
| A. Preparation     | — | Inspection strategy, scope, and inspection method            |
| B. Conducting      | — | Compile results, create feedback, develop improvements       |
| C. Post Inspection | — | Review documentation, observe processes, interview personnel |

### Lesson Conclusion

#### 1. Summary

In this lesson, you learned about the requirements for conducting security inspections and the broader purposes and importance of self inspections. You also learned the recommended three-step process for structuring self inspections.

## Answer Key

### Review Activity 1

	True	False
The NISPOM requires contractors to conduct a formal self inspection.	<input checked="" type="radio"/>	<input type="radio"/>
The NISPOM states that a government security inspection of all cleared contractor facilities will be conducted periodically.	<input checked="" type="radio"/>	<input type="radio"/>
DD Form 441 states that government representatives have the right to review facilities utilized by the contractor.	<input checked="" type="radio"/>	<input type="radio"/>
The NISPOM states that if a facility receives a rating of commendable or better, no self inspection needs to be performed.	<input type="radio"/>	<input checked="" type="radio"/>

### Review Activity 2

- 1) Your facility, which is inspected every twelve months, was last inspected by an IS Rep in March and received a rating of "Satisfactory." No other inspections have been conducted since then and it is now December. Would it be appropriate to conduct a self inspection?
- Yes, self inspections should be performed every three months.
  - No, facilities that receive a rating of Satisfactory or better do not need to perform self inspections.
  - Yes, self inspections should be performed midway between government inspections and it is now three months after the midway point.

*Since your facility is on a twelve month government inspection cycle and your last government inspection was in March, a self inspection was due in September. Although it is now 3 months overdue, you should still perform a self inspection.*

- 2) You were informed last Friday that one of the projects on which classified work is performed at your facility 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 incidents 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 his project specifically and not the facility in general.

*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.

*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

- |                           |              |  |
|---------------------------|--------------|--|
| <b>A.</b> Preparation     | <u>  A  </u> | Inspection strategy, scope, and inspection method            |
| <b>B.</b> Conducting      | <u>  C  </u> | Compile results, create feedback, develop improvements       |
| <b>C.</b> Post Inspection | <u>  B  </u> | Review documentation, observe processes, interview personnel |

# Student Guide

## **Course: NISP Self Inspection**

### ***Lesson 3: Preparing for Your NISP Self Inspection***

#### **Introduction**

##### **1. FSO Storyline**

*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, 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.*

##### **2. Objectives**

As with any project, self inspections require a great deal of planning and preparation. Here are the lesson objectives:

- 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**

##### **1. 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. What tasks related to the self inspection are you, the FSO, responsible for?*

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 project 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 the documents have been reviewed and all employee interviews have been completed. Analyzing the findings of an inspection and understanding when and how to revise your facility's security program accordingly is the responsibility of the FSO. Should a self inspection reveal any security

concerns, it is your responsibility to communicate those concerns to your government representative when it is appropriate to do so. 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 the inspection.

## **2. Roles of Other Participants**

NISP self inspections cannot be performed without the participation and cooperation of key individuals. 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.

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 procedures, ahead of time.

## **Developing an Inspection Strategy**

### **1. What is a Self Inspection Strategy?**

You should model your self inspection on the government security inspection. 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 by various identified inspection elements. Reviewing these elements will help you determine what to examine during your self inspection and what to verify about your security program as it relates to each applicable element.

In addition, you should develop an inspection strategy, to outline how you will 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. A self inspection strategy should also contain the following elements: administrative preparations and pre-inspection research. We will examine each of these elements more closely in the screens to follow.

### **2. Administrative Tasks**

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

#### **a. Select Dates**

You know that it is recommended that you perform a self inspection midway between government inspections. You, therefore, have a great deal of advance notice about when you need to conduct your self inspection. When determining the actual date or dates of the self inspection, be sure to consider: personnel 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.

**b. 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 inspections.

**c. Make an Announcement**

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.

*The information in the box below will not be on the test, but it may provide you with useful background and insights.*

**Sample 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. 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*

### **3. Pre-Inspection Research**

Part of conducting the self inspection involves reviewing various security records and conducting employee interviews.

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

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 topics you want to discuss with each individual. This will ensure your interview will remain focused on the inspection.

### **4. 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. The best way to use the handbook is to review the security elements and related questions and ask yourself which ones 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.

Conducting a self inspection requires much more than a simple paper check. You should do more than just locate the document that is required to be reviewed, you should actually review the information provided in each document, check company records and talk to company officials 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 interview your employees and, when possible, 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 policy and procedures, you can maintain a better awareness of your security program through them.

## 5. Applicable Inspection Elements

*Consider: Each facility is unique. Depending on the level of involvement your facility has in dealing with classified information and materials, 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?*

While the Self Inspection Handbook indicates three inspection elements that every facility must include in its self inspection, there are actually seven inspection elements that generally apply to all facilities. These seven elements are listed in the Self Inspection Handbook under:

- Element A, Facility Clearance
- Element B, Access Authorizations
- Element C, Security Education
- Element E, Standard Practice Procedures, if your facility has them
- Element G, Visit Control
- Element I, Classification
- Element K, Foreign Ownership, Control, or Influence, or FOCl.

Possessing facilities, or those facilities where classified information is received, stored and possibly generated, may need to include additional elements. There are seven additional elements that commonly apply to most possessing facilities. These seven elements are listed in the Self Inspection Handbook under:

- Element M, Classified Storage
- Element O, Markings
- Element P, Transmission
- Element Q, Classified Materials Controls
- Element R, Reproduction
- Element S, Disposition
- Element T, Information Systems.

This list is not all-inclusive. 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 seven elements common to all NISP facilities and six of the seven elements common to most possessing NISP facilities. No classified work is performed on an accredited information system at the facility, so element T, Information Systems, is not applicable at this time.*



## Inspection Methods

### 1. 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 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 closed areas 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. There are currently no computer systems used at your facility to process classified information.*
- *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 the 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, and the work for which is performed at this facility, is called "Axle." You decide to conduct your self inspection using this program.*

**a. Comprehensive Inspection Method**

It is recommended that periodically, all facilities perform a self inspection using the comprehensive method. The inspection can be divided up by business function or department, or by inspection element category.

**b. 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 1

*Which of the following activities are the responsibility or role of which party? Select FSO, Management, or Program Manager for each statement. Check your answers in the Answer Key at the end of this Student Guide.*

	<b>FSO</b>	<b>Management</b>	<b>Program Manager</b>
Recognize when it is appropriate to perform a self inspection.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Display support for, and allocate resources to, the self inspection.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Arrange appropriate interview times for personnel under his or her purview.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ensure the self inspection is conducted effectively.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

### Review Activity 2

*What activities are involved in preparing for a self inspection? Match each preparation activity category with the appropriate description. Check your answer in the Answer Key at the end of this Student Guide.*

- |                                   |     |  |
|-----------------------------------|-----|--|
| <b>A. Administrative</b>          | ___ | Use the Self Inspection Handbook to select inspection elements to be reviewed during inspection            |
| <b>B. Pre-Inspection Research</b> | ___ | Create a list of documents, create a list of personnel to interview and topics to discuss during interview |
| <b>C. Determining Scope</b>       | ___ | Select dates, secure management support, announce the inspection   |

### Review Activity 3

Which of the following inspection elements commonly pertain to which type of facility? Select “Most NISP Facilities” or “Most Possessing Facilities” for each statement. Check your answers in the Answer Key at the end of this Student Guide.

NISP Self Inspection Element	Most NISP Facilities	Most Possessing Facilities
Facility Clearance	<input type="radio"/>	<input type="radio"/>
Visit Control	<input type="radio"/>	<input type="radio"/>
Classified Materials Controls	<input type="radio"/>	<input type="radio"/>
Access Authorizations	<input type="radio"/>	<input type="radio"/>
Classified Storage	<input type="radio"/>	<input type="radio"/>
Markings	<input type="radio"/>	<input type="radio"/>
Security Education	<input type="radio"/>	<input type="radio"/>

### Review Activity 4

Given some characteristics about an inspection method, select the inspection method being described. For each question, select the best answer. Check your answers in 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

#### 1. Summary

In this lesson, you learned about the responsibilities of the FSO, and the roles of other organization team members, as they support the FSO in conducting a self inspection. You also learned about developing an inspection strategy to help you plan the actual execution of your self inspection. Finally, you learned the two primary inspection methods used to structure your inspection approach.

## Answer Key

### Review Activity 1

	FSO	Management	Program Manager
Recognize when it is appropriate to perform a self inspection.	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Display support for, and allocate resources to, the self inspection.	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Arrange appropriate interview times for personnel under his or her purview.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Ensure the self inspection is conducted effectively.	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

### Review Activity 2

- |                            |          |  |
|----------------------------|----------|--|
| A. Administrative          | <u>C</u> | Use the Self Inspection Handbook to select inspection elements to be reviewed during inspection            |
| B. Pre-Inspection Research | <u>B</u> | Create a list of documents, create a list of personnel to interview and topics to discuss during interview |
| C. Determining Scope       | <u>A</u> | Select dates, secure management support, announce the inspection   |

### Review Activity 3

NISP Self Inspection Element	Most NISP Facilities	Most Possessing Facilities
Facility Clearance	<input checked="" type="radio"/>	<input type="radio"/>
Visit Control	<input checked="" type="radio"/>	<input type="radio"/>
Classified Materials Controls	<input type="radio"/>	<input checked="" type="radio"/>
Access Authorizations	<input checked="" type="radio"/>	<input type="radio"/>
Classified Storage	<input type="radio"/>	<input checked="" type="radio"/>
Markings	<input type="radio"/>	<input checked="" type="radio"/>
Security Education	<input checked="" type="radio"/>	<input type="radio"/>

## 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

*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

*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.*

# Student Guide

## **Course: NISP Self Inspection**

### ***Lesson 4: Conducting Your NISP Self Inspection***

#### **Introduction**

##### **1. FSO Storyline**

*You did a great job creating your inspection strategy! While you were planning for your self inspection, you determined which inspection elements apply to Performance Basics based on its level of classified involvement and the work performed at the facility, and you determined the most appropriate inspection approach to be the programmatic approach.*

*Now you are ready to begin your self inspection. You will review records, interview personnel, 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 vice president, Edward Jamison, issued the announcement about your self inspection, you visited the closed area for project Axle and met with the employees who work on the project. You spoke with Jane Laramé, a senior business analyst, Cortney Herst, a junior business analyst, Steven Lawson, an assistant program manager Paul Velardi, an engineer, Fiona Johnson, an administrative assistant, and Lisa Renard, another administrative assistant.*

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

##### **2. 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:

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

##### **3. Lesson Overview**

Conducting a self inspection involves three basic activity areas:

- Reviewing security records
- Interviewing cleared employees
- Examining safeguarding systems

You review security records to validate that your security records are current and accurate. You conduct interviews to verify that cleared employees are aware of their

security responsibilities and understand the security requirements applicable to them as employees at a cleared facility. You examine safeguarding systems by inspecting safeguarding equipment and observing safeguarding procedures to verify that classified information is properly protected and 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.

## **Self Inspection Elements**

### **1. 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. Each element comprises a series of questions that address the basic 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. In addition to the Self Inspection Handbook and the NISPOM, you may want to use the Self Inspection Checklist provided by the Center for Development of Security Excellence. Now, let's look at some of the more common inspection elements in greater detail.

### **2. Common to All NISP Facilities**

As you learned in the previous lesson, there are seven inspection elements that apply to all cleared contactors or contractor facilities. All self inspections should cover:

- Element A, Facility Clearance
- Element B, Access Authorizations
- Element C, Security Education
- Element E, Standard Practice Procedures (if applicable)
- Element G, Visit Control
- Element I, Classification
- Element K, Foreign Influence, Control, or Ownership

Let's examine the intent behind each of these elements.

#### **a. Element A: Facility Clearance**

Element A relates to your Facility Clearance. 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, 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 e-FCL when appropriate.

**b. Element B: Access Authorization**

Element B is related to making sure the appropriate security procedures are completed in regards to personnel clearances. Are Joint Personnel Adjudication System or JPAS records regarding your cleared employees up to date? Have personnel security clearance applications been properly initiated and documented? Ensuring your personnel clearances are kept to the minimum ensures that only those employees actually working on classified projects have access to classified information.

**c. Element C: Security Education**

Element C asks whether appropriate security training and briefings have been provided to all cleared employees as required. Are the required security records available for verification? Element C also asks if cleared employees are appropriately debriefed when access to classified information is terminated. 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.

**d. Element E: Standard Practice Procedures**

Although not a NISPOM requirement for all cleared facilities, if your company has decided to implement Standard Practice Procedures or SPP, Element E applies. If you have an SPP, you must ensure that your procedures are in compliance with all applicable NISPOM requirements. Just as the NISPOM is continually updated, your facility's SPP should be updated to reflect those NISPOM changes that affect your security program.

**e. Element G: Visit Control**

Element G asks whether appropriate security procedures are in place to protect classified material during visits. Is each classified visitor's personnel clearance being verified? Are procedures in place to establish visitors' need to know for access to classified information? Are all classified visitors properly escorted? Visitors pose unique security concerns. Regardless of how familiar a classified visitor may be to your company or its employees, the requisite security procedures should be applied to every classified visitor, every time.

**f. Element I: Classification**

Element I relates to classification guidance as required by the DoD Contract Security Classification Specification, or DD Form 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.

**g. Element K: Foreign Ownership, Influence, or Control**

Element K applies to all contractors and relates to any material changes affecting the foreign ownership, control or influence, or FOCI, of your company. Have any of these changes occurred at your company? Have they been promptly reported to your Government Representative using e-FCL? 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 such decisions because they may affect your facility's continued capability to maintain its security clearance.

### **3. Common to Most Possessing NISP Facilities**

The seven elements we just examined are common 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 protect classified material, possessing facilities will need to include several additional inspection elements in the scope of a self inspection. These are only some of the inspection elements that commonly apply to possessing facilities. Your facility may be subject to additional inspection elements depending on your level of actual classified involvement. Let's examine the intent behind some of the inspection elements common to most possessing facilities.

Most NISP Possessing Facility self inspections should cover:

- Element M: Classified Storage
- Element O: Markings
- Element P: Transmission
- Element Q: Classified Materials Controls
- Element R: Reproduction
- Element S: Disposition
- Element T: Information Systems (if applicable)

#### **a. Element M: Classified Storage**

Element M asks whether the appropriate security procedures are in place for the storage or protection of classified information at your facility. 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?

#### **b. Element O: Markings**

Element O asks whether classified materials are properly marked. Is all classified material in your facility appropriately marked? The purpose of classification markings is to warn the holder that the information is, in fact, classified at a particular level and then to instruct the holder on the appropriate handling and protection requirements.

#### **c. Element P: Transmission**

Element P asks 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? You are

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

**d. Element Q: Classified Materials Controls**

Element Q helps to ensure that 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.

**e. Element R: Reproduction**

Element R relates to classified reproduction. The reproduction of classified materials should be kept to a minimum and should be documented appropriately. Is reproduction authorization obtained when required? Is a record of reproduction maintained when required? Copies require the same level of protection as originals so it is important to ensure that all copies are reviewed to verify that classification markings were not lost during the reproduction process.

**f. Element S: Disposition**

Element S asks whether there are effective processes in place to facilitate the retrieval, declassification, and destruction of classified material at your facility. Are appropriate records being maintained, when required? The disposition of classified information comprises many different activities. Your cleared employees should be aware of how to properly engage in each activity and when and how to document their actions.

**g. Element T: Information Systems**

Element T applies if your organization has accredited information systems used to process classified information. Are the certifications for the information systems up to date? Are appropriate procedures implemented to maintain the security of the information systems? Are required records and logs being maintained? A significant portion of security violations involve the misuse of information systems. Many times, employees are simply unaware of the security policy regarding information systems, or they didn't realize that their action constituted a security violation.

*The information in the box below will not be on the test, but it may provide you with useful background and insights.*

**Accredited Information Systems**

Be sure to make your cleared employees aware that all information systems used to process classified information must first be accredited by the CSA. Once the system is accredited, 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

### 1. Record Selection

Part of conducting the self inspection involves reviewing various security records and conducting employee interviews.

*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 Government Representative 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, KMP list, SF-328 and employees' SF-86s. Other records, such as those related to accredited information systems may not apply depending on your organization's level of classified involvement.

#### a. Common Security Records

Here is a listing of security records that you may need to review in the course of your inspection. This listing of records is based on the questions listed under each of the Security Elements in the Self Inspection Handbook and is not intended to be all-inclusive.

*This listing of security records is based on the questions listed under each of the Security Elements in the Self Inspection Handbook and **is not intended to be all-inclusive.***

#### Element A: Facility Clearance

- DD Form 441 and/or 441-1
- KMP List
- SF 328
- DSS Form Letter 381-R

#### Element B: Access Authorizations

- SF 86, signed releases until eligibility has been granted

#### Element C: Security Education

- SF 312 (not required to be maintained)
- Special briefings
- Refresher briefings
- Refusal to execute SF 312

**Element D: Consultants**

- Consultant certificates

**Element E: Standard Practice Procedures (SPP)**

- Standard Practice Procedures

**Element F: Subcontracting**

- DD Form 254

**Element I: Classification**

- DD Form 254
- Classification Guide(s)

**Element J: Employee Identification**

- ID cards/badges for couriers/hand carriers/escorts
- Written assurance from manufacturer of automated access control devices that the devices meet NISPOM 5-313 standards

**Element K: Foreign Ownership, Control, or Influence**

- SF 328
- FOCI Negation Plan, if required
- National Interest Determination (if cleared under a Special Security Agreement)
- Technology Control Plan, if required
- Annual Implementation and Compliance Report, if required

**Element L: Public Release**

- Requests for Release

**Element M: Classified Storage**

- DSS approval for the open storage of documents in any closed areas
- Record of the names of people having knowledge of security container combinations
- Signed & dated Certificates of Repair

**Element N: Controlled Access Areas**

- Approval of FSO for the installation of any Supplanting Access Control Systems
- DSS approvals for Intrusion Detection Systems that do not meet NISPOM or UL 2050 standards
- UL 2050 CRZH certificate(s)

**Element P: Transmission**

- Receipts of classified transmissions

**Element R: Reproduction**

- Record of reproduction for TS materials

**Element S: Disposition**

- Retention Authority requests
- Records of Destruction for TS materials

#### **Element T: Information Systems**

- DSS Written Accreditation for the SSP (or Interim Approval), ISSM Authorization of Self-Certification Authority
- Notification from the ISSM to DSS of IS Certifications
- IS Accreditation
- IS Security Policy
- Protection Level Authorization
- Maintenance logs reflecting changes in hardware configuration
- Proof of compliance with construction requirements if IS located in closed area
- Approval for open storage of classified information, media, or equipment
- Proof of compliance with PDS construction requirements
- Inspection log of transmission lines not in a PDS if closed area has false ceilings/floors
- Record of all appropriate audit entries
- Protection Requirements for each audit requirement
- ISSM approval for the use of maintenance tools and diagnostic equipment

#### **Element U: COMSEC/CRYPTO**

- See NSA/CSS Policy Manual No. 3-16, November 2005

#### **Element V: International Operations**

- Export Authorizations for the disclosure of classified information
- Requests for export authorization (accompanied by DSP-83 if significant military equipment/classified material)
- Subcontract document for all direct commercial arrangements with foreign contractors involving classified information
- Transportation Plan for contracts involving international transfer of classified material as freight
- Hand Carry Plans for contracts involving international transfer of classified material via cleared courier(s)
- Courier Certificate(s)/Courier Declaration(s)
- Technology Control Plan for controlling access to all export controlled information
- Requests for visits abroad
- Appropriate certificates and records for briefings/debriefings of employees accessing NATO classified materials
- Accountability records for NATO classified materials as required
- Record of visit for persons representing NATO

## **2. Examining Records**

*Knowing how to effectively verify security records is essential to conducting an accurate and efficient self inspection. Consider: Some aspects of your security program such as your personnel security clearances or classified holdings can become quite extensive. This creates a large number of the same type of security record. How would you approach trying to review so many records?*

One technique used to examine a large quantity of the same type of security record is called sampling. As the name suggests, this technique involves reviewing a sampling of the same type of security record, instead of reviewing every single instance of the record. 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.

One technique you can use to verify and validate information contained in security records is through forward and reverse checks. Forward checks begin by reviewing the security record 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 through these activities by confirming it in the contents of a security record.

#### **a. Sampling**

Recall that some documents, for example personnel security clearances, are used by a wide variety of individuals and programs, creating 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.

When reviewing security records of this nature, it is acceptable to implement a technique called sampling. Sampling is a technique that involves selecting and reviewing a random sample of the security record being examined. You can then use the results of this sample review to extrapolate a general status about how that security record is being maintained.

#### **b. Forward and Reverse Checks**

One technique you may use when verifying the information contained in a security record is called forward or reverse checks. When conducting a forward check, you begin by gathering relevant information from a security record. Once you have gathered the relevant information, you then verify that information by examining the security procedures in place relevant to the information.

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. You begin by examining classified material, interviewing an employee, or observing a security procedure and then verify your findings from these activities by reviewing appropriate security records relative to the findings.

### **3. 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.*

#### **a. Element A: Facility Clearance**

*While reviewing security records related to the requirements under Element A, Facility Clearance, you found that Performance Basics' Department of Defense Security Agreement, or DD Form 441; Certificate Pertaining to Foreign Interests, or SF-328; and Letter of Notification of Facility Clearance, or DD Form Letter 381-R; are all present, complete, and up to date. Upon reviewing Performance Basics' Key Management Personnel Listing however, you found that the recent change to the Board of Directors was not reported.*

**b. Element B: Access Authorizations**

*You reviewed personnel clearances as part of your inspection related to requirements under Element B, Access Authorizations, and found that an employee, Spencer Richards, has an active clearance despite the fact that the classified project he was working on was completed four months ago.*

**c. Element C: Security Training**

*A review of the security training records at Performance Basics revealed that initial security briefings for all newly 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.*

**d. Element I: 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.*

**e. Element K: Foreign Ownership, Control, or Influence**

*Security records, confirmed by interviews with senior management, related to requirements under Element K, Foreign Ownership, Control, or Influence, or 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 inspection.*

## **Employee Interviews**

### **1. 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 inspection.*

Cleared employees will comprise the majority of the individuals you will interview during a self inspection. 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.

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.

#### **a. General Questions**

Some questions should usually be asked of every interview candidate. You should always assess whether the candidate is aware of the security responsibilities attributed to them. You should typically determine if the interview candidate has, or is in the process of applying for, a security clearance and then inquire about the status of their clearance or application for clearance. Particularly for uncleared interview candidates, you should always inquire whether they have had any access to classified areas, information, or materials.

General Questions:

- Is the interview candidate aware of the security responsibilities attributed to them as a cleared/uncleared individual?
- Does the interview candidate have a clearance or an application for clearance pending?
- Is their clearance or application for clearance up to date and in good order?
- Is the interview candidate able to access classified areas, information, or materials?

## **2. 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. Review each of the techniques to learn how to implement them and make your employee interviews more successful.

#### **a. 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 he had been involved in a security violation in the past twelve months, he 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 unaccredited 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 the following examples of leading questions and see if you can determine what the question is leading the responder to reply with.

**Q1.** Of course, you always conduct your end of day security check before leaving work every day, right?

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

**Q2.** You didn’t use your badge to let your coworker, who forgot his badge, inside the secured area, did you?

*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.*

**Q3.** You would never discuss classified information with someone who didn’t have a need-to-know, would you?

*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. Open-ended questions are 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 an open-ended question is “Could you please describe the process you follow when you access classified information on your accredited computer?” This question requires the responder to explain the procedures he or she follows when working on one of the company’s accredited information systems. From the response, you can determine if the individual is forgetting a key aspect of the security measures related to information systems.

#### **b. 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. The good notes that you take, will assist you in assessing the results of your self inspection.

When you ask open-ended questions, you will find that most people feel compelled to reply with a complete story. Individuals may 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 interview candidates 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 with the candidate. 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.

### **c. 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 program.

By observing your security procedures in action, you may find a more efficient or effective way to accomplish a task that you might want to incorporate into your company's security procedures.

### **3. Practical Exercise: Cortney Herst**

*Apply your understanding of employee interview techniques. Cortney 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.*

- 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?
- 2) When you generate classified documents for this project, you place the markings at the top, bottom, front, and back of each page, correct?
- 3) Could you please demonstrate how you apply classification markings to the classified documents you generate for this project?

*Option one 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 two 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 three 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.*

**a. Results for Courtney Herst**

**FSO:** “Could you please demonstrate how you apply classified markings to the classified documentation you prepare for this project?”

**Ms. Herst:** “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.”

*Ms. Herst responded that she always applies classification markings on any of the classified material she prepares. She marks each document by stamping “Top Secret” on the cover page of the document only. 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 self inspection Element O, Markings.*

**4. Practical Exercise: Steven Lawson**

*Apply your understanding of employee interview techniques. Steven Lawson is a senior contracting officer who coordinates client site operations with work performed at your facility for project Axle. You need to verify that he understands the requirements regarding visitor escorts, and that he implements those requirements appropriately. Select the most appropriately phrased question to ask Mr. Lawson.*

- 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?
- 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?
- 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?

*Option one asks Mr. Lawson to explain how he handles a classified visitor at your facility. This is the most appropriate question as it allows Mr. Lawson to explain all that he knows about the topic without prompting him to reply with a particular response.*

*Option two asks Mr. Lawson a series of yes or no questions, limiting his replies to only those aspects of the topic that you thought to ask about.*

*Option three asks Mr. Lawson about implementing visitor escort requirements using a leading question, prompting him to reply with the response he knows you would like to hear, rather than with his own knowledge about the topic.*

**a. Results for Steven Lawson**

**FSO:** “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?”

**Mr. Lawson:** “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.”

*Mr. Lawson responded that he is designated as the escort for this project and has received extra training about his responsibilities. He indicated that he receives visitors and escorts them while they are visiting. Mr. Lawson’s response should be noted under self inspection Element G, Visit Controls.*

**5. Results: Paul Velardi**

*Paul Velardi is an engineer who provides support to client-side research initiatives. If your company has a Standard Practice Procedures guide, you need to verify that it is up-to-date, that it includes all required security procedures, and that it is available to all cleared employees working on the project.*

**FSO:** “Could you please clarify if this facility has Standard Practice Procedures and describe how such guidance may be accessed by project personnel?”

**Mr. Velardi:** “Yes, we have Standard Practice Procedures. A hard copy is maintained by the program manager’s administrative assistant. She works with the FSO to ensure updates to procedures are incorporated and team members can access it any time they need to.”

*Mr. Velardi responded that there is a Standard Practice Procedures guide for this facility and that cleared employees working on project Axle can review these procedures at any time from a hard copy kept by the administrative assistant. Mr. Velardi’s response should be noted under self inspection Element E, Standard Practice Procedures.*

**6. Results: Fiona Johnson**

*Fiona Johnson is an administrative assistant supporting a variety of work performed for project Axle. You need to verify that she understands the requirements regarding the destruction of classified documents, and that she implements those requirements 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?”

**Ms. Johnson:** “Oh, yes, when I am notified that SECRET documents need 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 responded that when she is notified that SECRET documents need to be destroyed she takes the documents and places them in the cross-cut shredder. She indicated once the documents have been shredded, she looks through the clippings to make sure the material was properly shredded. Ms. Johnson’s response should be noted under self inspection Element S, Disposition.*

## **Safeguarding Systems**

### **1. 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 designated cleared employees as they perform end of day security checks.

Reviewing any 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.

### **2. Safeguarding Systems Results**

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

#### **a. Element M: Classified Storage**

*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.*

**b. Element N: Controlled Access Areas**

*You observed the access controls in place for accessing the area where work on this project is performed. A cleared employee used their badge, which is programmed with the access privileges to enter this area and their personal identification number, to open the door. The cleared employee's name appears on the authorized access list.*

**c. Element P: Transmission**

*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 closed area for this project, and stored the contents of the package in one of the security containers.*

## Review Activity 1

*What activities are involved in conducting a self inspection? Match each category of activities to the appropriate description of activities performed. Check your answer in the Answer Key at the end of this Student Guide.*

- |                                 |   |   |
|---------------------------------|---|---|
| A. Review Security Records      | — | Observing a demonstration of actual procedures being implemented                                |
| B. Employee Interviews          | — | Sampling technique, forward check, reverse check  |
| C. Examine Safeguarding Systems | — | Asking open-ended questions and listening to the respondent's story, asking for a demonstration |

## Review Activity 2

*Given a description of a record verification technique, identify which technique is being discussed. For each question, select the best answer. Check your answer in the Answer Key at the end of this Student Guide.*

- 1) Review a security record, then confirm the record's contents 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 findings of these activities 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. For each question, select the best answer. Check your answer in the Answer Key at the end of this Student Guide.*

- 1) Because the responder 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 responder 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

#### 1. Summary

In this lesson, you learned about the self inspection elements common to all NISP facilities, and those common to most possessing facilities based on level of classified involvement. You also learned about the three primary activities involved in conducting a self inspection. Finally, you learned techniques to help you conduct each of the three primary activities.

## Answer Key

### Review Activity 1

- |                                 |          |   |
|---------------------------------|----------|---|
| A. Review Security Records      | <u>C</u> | Observing a demonstration of actual procedures being implemented                                |
| B. Employee Interviews          | <u>A</u> | Sampling technique, forward check, reverse check  |
| C. Examine Safeguarding Systems | <u>B</u> | Asking open-ended questions and listening to the respondent's story, asking for a demonstration |

### Review Activity 2

- 1) Review a security record, then confirm the record's contents by conducting employee interviews, observing procedures, and examining physical security components.
- Sampling
  - Forward Checks
  - Reverse Checks

*Forward checks begin with reviewing a security record followed by verifying the record's contents 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 findings of these activities by reviewing security records.
- Sampling
  - Forward Checks
  - Reverse Checks

*Reverse checks begin with activities such as employee interviews, observing procedures, or examining physical security components followed by reviewing security records to verify the findings of those activities.*

### Review Activity 3

1) Because the responder 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

*Asking open-ended questions avoids limiting the respondent's reply to only the information a single-answer question, such as a "yes/no" question, would provide. This technique also avoids prompting the respondent 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

*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 responder 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

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

# Student Guide

## Course: NISP Self Inspection

### Lesson 5: After Your NISP Self Inspection

#### Introduction

##### 1. FSO Storyline

*That was a lot of work, good job! You completed your review of required documents, conducted personnel interviews with key members of 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 inspection.*

##### 2. Objectives

In this lesson, we will learn how to make use of the results from your inspection. You will learn about post inspection activities such as developing your inspection results, creating feedback, and determining what follow-up actions, if any, you should take. Here is the lesson objective:

- Identify the actions involved in conducting post self inspection activities

#### Compiling Self Inspection Materials

##### 1. Results

*Before you can begin reviewing the results of your inspection, you should compile and organize all the documentation related to the inspection. You will want to collect the documentation you compiled as research and preparation materials, your self inspection strategy, and your notes from the inspection. Using these materials, you can develop your inspection findings. Here are the findings from your self inspection, organized by inspection element. Review each inspection element to see the finding associated with it.*

**Element A, Facility Clearance:** A review of security records revealed that DD Form 441, SF-328, and DSS Form 381-R are all present, completed, and up to date. The Key Management Personnel List, however, does not appear to be up to date.

**Element B, Access Authorizations:** A review of security records revealed that employee Spencer Richards has an active clearance, however the project he was working on that required him to have access to classified material was completed four months ago.

**Element C, Security Education:** 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.

**Element E, Standard Practice Procedures:** When interviewed, Paul Velardi indicated that he is aware that the facility has Standard Practice Procedures, a copy of which is maintained by the program manager's administrative assistant and is accessible to all employees at any time.

**Element G, Visit Control:** When interviewed, Steven Lawson indicated that he was aware of his responsibilities as the escort for visitors working on project Axle and that he received extra training for his duties as an escort. He indicated that he receives visitors, verifies their identity and clearance level and escorts them while they are visiting.

**Element I, Classification:** A review of security records revealed that a DD Form 254, Contract Security Classification Specification, is on file for all classified contracts held at this facility. Classification guidance is available and is challenged when necessary

**Element K, Foreign Ownership, Control, or Influence:** A review of documents revealed that the company's SF-328, Certificate Pertaining to Foreign Interests, is present, up to date, and matches the copy your Government Representative has on file.

**Element M, Classified Storage:** You examined each of the security containers used for project Axle and determined that all the security containers are in good order. You validated the procedures followed when performing an end-of-day security check and determined the procedure to be correct.

**Element N, Controlled Access Areas:** You observed the access controls in place for accessing the closed area where work on project Axle is performed. A cleared employee uses their badge, which is programmed with the access privileges to enter the area and enters their personal identification number to open the door. The cleared employee's name appears on the authorized access list.

**Element O, Markings:** When interviewed, Cortney 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 implementing page and portion markings on the classified material that she generates.

**Element P, Transmission:** 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 contents of the package in one of project Axle' security containers.

**Element S, 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

## 2. Self Inspection Results

Self inspection results comprise more than just your findings. 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 may want to maintain a copy of the Self Inspection Certificate you send to your IS Rep upon completing your self inspection.

## Developing Self Inspection Feedback

### 1. Feedback

*Consider: Review your notes from your 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 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 finding, and a brief explanation about how the result was determined. 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: via a company newsletter, in an email distributed to all employees, by giving a briefing, or in training sessions. Feedback should be directed to management and employees at your facility, as well as your government representative, when necessary. When creating your feedback, structure it according to the recommended sequence of topics:

- 1) Identify any positive observations first to include any employees who were exceptional in carrying out their security responsibilities
- 2) Then, identify any findings or areas needing improvement.
- 3) Following that, provide corrective actions for those findings.
- 4) 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. In addition, your feedback should detail those results that require corrective action.

*The information in the box below will not be on the test, but it may provide you with useful background and insights.*

#### **Sample Self Inspection Feedback:**

*Positive observations:*

- *Procedures for the handling of incoming classified visitors to the facility*
- *Transmission procedures for the receipt of classified packages*

*Four findings requiring corrective action:*

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

## Following Up After a Self Inspections

### 1. Follow-Up Activities

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

Once you have determined what the results of your 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. 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 documentation, such as a Key Management Personnel List, has been updated for completion or accuracy and is 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 to incorporate 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, implementing the corrective actions necessary to address the concern and thereby ensuring 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.

*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 Vice President of the company, Mr. 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.*

*Remember that you discovered that Spencer Richards has an active clearance even though the project he was working on that required the clearance was completed four months ago. To address the inconsistency between active personnel clearances and the projects requiring cleared personnel, you will work with program managers to reconcile active personnel clearances with the actual number of clearances needed to perform work on classified projects at your facility.*

*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 the requirements outlined in the NISP agreement.*

*To address the non-compliant practices regarding classified markings, you should emphasize this aspect in your security training.*

## **Conclusion**

*Congratulations! You compiled your inspection results, created feedback based on the findings from your inspection, and determined appropriate follow-up activities. You should now be familiar with your facility's security program. You have recommended to management that you would like to create an updated security education training program addressing some of the concerns revealed by your inspection, to present next month. You have provided Mr. Jamison with a guide outlining what types of changes to the organization might impact your facility's security clearance, and he has promised to inform you of any changes to the organization that you need to know about as the FSO.*



## Review Activity 1

*Self inspection results comprise which of the following? Select all that apply. Check your answers in the Answer Key at the end of this Student Guide.*

- Pre-inspection research and preparation materials
- Self inspection strategy
- Self inspection notes
- Self inspection findings and the interpretation of those findings
- Follow-up record
- Updated security policy
- Updated security training manual

## Review Activity 2

*What do you know about feedback? For each question, select all that apply. Review the answer key at the end of this student guide to check your responses.*

1) Your feedback should include which of the following?

- Positive findings
- Negative findings
- Solutions and improvements
- Thank yous

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

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

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

- Management
- Facility personnel
- IS Rep
- Vendors

### Review Activity 3

*Read each statement about follow-up activities, then determine if the statement is true or false. Check your answers in the Answer Key at the end of this Student Guide.*

- 1) The purpose of follow-up activities is to ensure that corrective actions or improvements recommended in response to 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

### Lesson Conclusion

#### 1. Summary

In this lesson, you learned about the elements that comprise self inspection results. You learned what information to include in your self inspection feedback, different forms of delivering your feedback, and who the recipients of your feedback are. You also learned about the purpose of follow-up activities and the different types of follow-up activities.

## Answer Key

### Review Activity 1

- Pre-inspection research and preparation materials
- Self inspection strategy
- Self inspection notes
- Self inspection findings and the interpretation of those findings
- Follow-up record
- Updated security policy
- Updated security training manual

### Review Activity 2

- 1) Your feedback should include which of the following?
  - Positive findings
  - Negative findings
  - Solutions and improvements
  - Thank yous
  
- 2) Which of the following forms of transmission are appropriate to use for your feedback?
  - Newsletter
  - File folder in the security office
  - Email
  - Training session
  
- 3) Recipients of your feedback may include which of the following?
  - Management
  - Facility personnel
  - IS Rep
  - Vendors

### Review Activity 3

- 1) The purpose of follow-up activities is to ensure that corrective actions or improvements recommended in response to 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

## Student Guide

### **Course: NISP Self Inspection**

#### ***Lesson 6: 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.

Performing a self inspection involves three stages: preparing for your inspection, conducting your inspection, and post-inspection activities. You should now understand how to use the Self Inspection Handbook in conjunction with the 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 activity categories involved in conducting a self inspection. 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.

You should now know that to protect your facility and its information and personnel, you must be aware of the types of threats that exist and how your adversaries operate. You must seek out and obtain threat information from a variety of sources and it is essential that you report threats that you encounter.

##### **Lesson Review**

Here is a list of the lessons in the course:

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

## Course Objectives

You should now be able to:

- ✓ 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

## Conclusion

Congratulations. You have completed the NISP Self Inspection course. To receive course credit, you *MUST* take the NISP Self Inspection examination. Please use the ENROL system from the Center for Development of Security Excellence to register for the online exam.