Visits and Meetings in the NISP

Student Guide

July 2021

Center for Development of Security Excellence

Table of Contents

Lesson 1: Course Introduction

Course Introduction

Course Information

Welcome to Visits and Meetings in the NISP Course. For more information about this course, or to view or print the Student Guides, select one of the available options. Select the forward arrow to proceed with the course.

Purpose: Provide a thorough understanding of the National Industrial Security Program (NISP) policy requirements to conduct visits and meetings in support of a Government Contracting Activity (GCA) that entails disclosure of classified information

Audience: Contractor Facility Security Officers, Security staff of cleared DOD contractors participating in the NISP, DCSA Industrial Security Representatives (IS Reps), and DOD Industrial Security Specialists

Pass/Fail %: 75% on final examination

Estimated: 120 minutes

Lesson Overview

Contractors and government employees working on classified programs and projects have occasions to visit one another's facilities and to gather at conferences and other arranged meetings. There is a distinction in the National Industrial Security Program Operating Manual, or NISPOM, between "visits" and "meetings". Although a classified visit is often called a classified meeting, it is important for you to know that they are not the same and have very different NISPOM requirements.

In this course, you will first learn about classified visits and then we will turn your attention to classified meetings in a later lesson. Visits and meetings that involve disclosure of classified information require security professionals to understand the procedures in the National Industrial Security Program, or NISP, and to implement the prescribed security controls to safeguard our nation's sensitive information. At times, personnel from your organization may be going to a classified visit or meeting. At other times, your organization will be hosting people at your facility.

Different responsibilities apply when sending visitors versus receiving visitors for classified visits and meetings. Keep in mind that classified visits and meetings may take place in the U.S. or abroad, but there are different requirements for domestic versus international visits. The requirements set forth in the NISPOM will help you understand these roles and responsibilities. This course will help you understand the NISP visit and meeting requirements, the necessary procedures and authorizations, and the roles of both visitor and host organizations in preparing for, and participating in, classified visits and meetings.

Course Objectives

Here are the course objectives:

- Identify the requirements for classified visits in the National Industrial Security Program (NISP)
- Identify the authorization responsibilities and procedures when sending an employee on a classified visit
- Identify the authorization responsibilities and procedures when hosting a classified visit
- Describe how to verify a visitor's identity and access
- Identify security briefing topics for visitors
- Recognize access controls appropriate for a classified visit
- Identify procedures for recovering classified material after a visit
- List best practices for maintaining security controls during visits
- Identify the requirements and security controls for incoming and outgoing international visits
- Describe the process for international visit approval including the role of the contractor, embassy, and Foreign Visits System (FVS)
- Identify the requirements and security controls for North Atlantic Treaty Organization (NATO) visits
- Recognize responsibilities of the Government Contracting Activity (GCA) in sponsoring classified meetings
- Indicate steps involved for a contractor to host GCA-sponsored meetings
- Identify security control responsibilities for hosting a classified meeting

Course Structure

This course is organized into the lessons listed here:

- Course Introduction
- Visit Basics
- Procedures for Classified Visits
- Security Controls during Visits
- International and NATO Visits
- Classified Meetings
- Course Conclusion

Lesson 2: Visit Basics

Introduction

Industry and government workers supporting a classified contract may have to visit one another's facilities to discuss the project. An important aspect of your role as a Facility Security Officer, or FSO, or as a member of your organization's industrial security staff, is understanding who is permitted to attend and what the requirements and procedures are for these visits. The National Industrial Security Program Operating Manual, or NISPOM, provides the requirements you will need to follow in carrying out your duties. In this lesson, you will learn the basic concepts and requirements for visits in the NISP.

Objective

- Identify the requirements for classified visits in the NISP

NISPOM: National Industrial Security Program Operating Manual.

Basic Concepts

Characteristics of Classified Visits

You will find the classified visit requirements in the NISPOM. The purpose of a classified visit is to share classified information between two or more people.

Classified visits may take place at a cleared contractor facility or at a federal facility and the intent of the visit must be for a lawful and authorized U.S. Government purpose. Although the participants may consider these meetings and even refer to them as such, they are not technically meetings within the definition of the NISPOM.

Characteristics of Classified Visits:

- Involve disclosure of classified information between two or more people
- Serve a lawful and authorized U.S. Government purpose

Visits have requirements for the disclosure of classified information!

Who Is a "Visitor" in the NISP?

Does a classified visit necessarily involve access to classified information? In theory, the answer is YES. However, under certain circumstances, the visit itself may not require access to classified information, but the visitor cannot be isolated from classified information in the cleared facility. For example, a maintenance person may have to enter a secure area in order to repair a piece of equipment that cannot be removed. The best way to deal with this would be to sanitize that area of all classified material and have a cleared employee escort that person to prevent him or her from having access to classified information. In some cases, the nature of the repair could mean that it is not possible to take these

measures. If a visitor cannot be excluded from access, then the visit must be handled as a classified visit, and all relevant requirements in the NISP must be met.

In some situations, a non-cleared person may be escorted by a cleared person in a secure area, such as when cleaning the office area is required. The escort must be properly cleared and must have enough knowledge of what is classified to prevent the uncleared person from having access to classified information. Escort policies differ from one facility to the next, so be sure you are familiar with them if this situation applies to you.

Who is a "visitor" in the NISP?

- An individual who is authorized to access classified information for a government purpose
- An individual who:
  - Needs access to a closed, classified area
  - Cannot be isolated from classified information

Visit Duration and Requirements

Visits may be a one-time event, may be intermittent over a period of time, or may be long-term. A one-time event visit would have a very specific duration such as for one particular day or consecutive days. Intermittent visits occur when a government employee or contractor needs to enter a cleared contractor or government facility intermittently for the duration of the contract or a specified period of time such as over a six month or one year timeframe. Long-term visits occur when the contractor employee stationed at another contractor's cleared facility or government facility. Long-term visits may also require frequent visits to the cleared facility, which may continue for the life of the contract.

Regardless of the visit duration, all visitors, whether government employees or contractors, must follow the security procedures of the host organization. For long-term visitors, the NISPOM provides additional clarification. Even though a contractor employee must follow the security requirements when visiting a government facility, this does not relieve the visitor's organization from continued security oversight of that employee. Government personnel assigned to or visiting a contractor facility and engaged in oversight of an acquisition program will retain control of their work products. Such personnel do not have to relinquish control of their work products to the contractor.

NISPOM: National Industrial Security Program Operating Manual.

NISP Requirements for Classified Visits

Determining Authorization

In order for a visitor to be permitted access to classified information during a visit, that visitor must be an authorized person. An authorized person is one who has obtained a favorable national security eligibility determination (also referred to as a Personnel Security Clearance, or PCL), at the required level. This may also be referred to as eligibility and access. The person must also have a need-to-know for the classified information in the

performance of official duties. The need-to-know determination is made by an authorized holder of the classified information that the visitor has a requirement for access to, knowledge, or possession of the information to perform tasks or services essential to the fulfillment of a classified contract or program.

Requirements for an Authorized Person:

NISP terminology:
- Personnel Security Clearance (PCL)
- Need-to-know

DOD Personnel Security System of Record terminology:
- Eligibility
- Access
- Need-to-know

NISP: National Industrial Security Program
Personnel Security Clearance: the administrative determination that an individual is eligible, from a security point of view, for access to classified information of the same or lower category as the level of the Personnel Security Clearance being granted
DOD Personnel Security System of Record: System of record for personnel security, suitability and credential management of all DOD employees, military personnel, civilians, and contractors.

Need-to-know

A person has a need-to-know when they need access to, knowledge of, or possession of classified information to perform tasks or services essential to the fulfillment of a classified contract or program. The determination of an individual's need-to-know rests with the entity disclosing the information. This determination is generally based on a contractual relationship, as documented in the DD Form 254.

Need-to-know:
- Requirement for access to, knowledge of, or possession of, classified information
- Information is essential to performance on a classified contract or program
  - Determination made by disclosing individual based on a contractual relationship
    - Documented in the DD Form 254.

NISPOM: National Industrial Security Program Operating Manual (NISPOM)
DD Form 254: Department of Defense Form 254 (DD Form 254) - Contract Security Classification Specification

Additional NISP Requirements

The NISPOM provides the key requirements for classified visits. The number of classified visits must be limited to the minimum needed to do a job. This is not only better from the government's standpoint of safeguarding classified information, but also makes your job easier if there are fewer classified visitors to track. Both the visitor's organization and the host organization must determine that the visit is necessary in the interest of national security *and* that the purpose of the visit cannot be achieved without access to, or

disclosureof, classified information.

In order for a visit request to be approved, the host organization must ensure that the visitor's identity is confirmed and has the proper PCL and need-to-know prior to the disclosure of any classified information. The host organization is responsible for ensuring that visitors are only given access to classified information consistent with the purpose of the visit. The host organization's approval of the visit constitutes authority for disclosure. Some classified visits may be by government representatives.

Government Representative Visits

Representatives of the Federal Government, when acting in their official capacities as inspectors, investigators, or auditors, may visit a contractor's facility. These representatives may be executing duties for a variety of agencies. These representatives must present appropriate government credentials upon arrival.

Review Activities

Check your answers in the Answer Key in Appendix A of this Student Guide.

Review Activity 1

Read each statement and determine if it is true or false.

1 of 3: Regardless of the visit duration, all visitors, whether government employees or contractors, must follow the host organization's security procedures.

- ○ True
- ○ False

2 of 3: When a contractor employee visits a government facility, he or she must follow the security requirements of that facility and the visitor's organization is relieved from continued security oversight of that employee.

- ○ True
- ○ False

3 of 3: Government personnel assigned to or visiting a contractor facility and engaged in oversight of an acquisition do not have to relinquish control of their work products to the contractor.

- ○ True
- ○ False

Review Activity 2

What are the key requirements for a classified visit in the NISP? *Select all that apply.*

- ☐ Visits must be held to a minimum.
- ☐ The visitor must certify that access is consistent with the purpose of the visit and show positive identification.
- ☐ The purpose for the visit must be in the national interest and cannot be achieved without access to classified information.
- ☐ The contractor must ensure the visitor has a Personnel Security Clearance (PCL) and need-to-know and provides positive identification.

Review Activity 3

The purpose for a classified visit in the NISP is to share classified information for a lawful and authorized U.S. Government purpose. *Select the best response.*

- ○ True
- ○ False

Review Activity 4

Which of the following are the visitor's authorization requirements for accessing classified information? *Select all that apply.*

- ☐ The authorized person must have been granted a Personnel Security Clearance (PCL) at the required level.
- ☐ The authorized person must have been granted access at a higher level than the host organization's Facility Clearance (FCL).
- ☐ The person must have a PCL at the required level, but a need-to-know determination is not required unless the information is Top Secret.
- ☐ The authorized person must have a need-to-know the classified information in the performance of official duties.

Review Activity 5

Which of the following are responsibilities of a host organization during a classified visit? *Select all that apply.*

- ☐ Determine that the visit is necessary in the interest of national security.
- ☐ Request disclosure authority from the visitor's organization.
- ☐ Determine that the purpose of the visit cannot be achieved without access to, or disclosure of, classified information.
- ☐ Ensure that the visitor's identity is confirmed and he or she has the proper PCL and need-to-know.

Lesson 3: Procedures for Classified Visits

Introduction

When a classified visit occurs, there are procedures for both the visitor's organization and the host organization to follow. These procedures can be found in the NISPOM. In this lesson, you will learn about the authorization methods for visits in the NISP as well as the procedures that visitor and host organizations must follow.

Objectives

Here are the lesson objectives:

- Identify the authorization responsibilities and procedures when sending an employee on a classified visit
- Identify the authorization responsibilities and procedures when hosting a classified visit

NISPOM: National Industrial Security Program Operating Manual

Authorization Methods

DOD Personnel Security System of Record

If a visit requires access to classified information, the visitor organization submits a visit authorization request. Verification of a visitor's PCL may be accomplished by a review of an individual's information in the DOD Personnel Security System of Record, which provides real time information about the PCL, or by a Visit Authorization Letter, or VAL, provided by the visitor's employer. If the DOD Personnel Security System of Record is not available, a VAL is required to be provided to the host by the visitor's employer. The DOD Personnel Security System of Record provides real-time eligibility determinations and investigative status to authorized security personnel. It must be used to decide whether a person may be granted access to classified information. The system is used by FSOs and designated security personnel, DCSA IS Reps, and other DOD agencies. Contractors are responsible for annotating and maintaining the accuracy of their employees' access records in the DOD Personnel Security System of Record.

Eligibility: The highest level of information which may be disclosed to a person based on the type of completed and favorable investigation. It is a CAF responsibility to assign eligibility.
Access: The actual level of classified information to which a person is authorized disclosure. It is a security officer's responsibility to assign access level.
FSO: Facility Security Officer
DCSA IS Rep: Defense Counterintelligence and Security Agency Industrial Security Representative
NISPOM: National Industrial Security Program Operating Manual

VAL Method

The alternate method for a visit authorization is the VAL, which is provided by the visitor's organization. VALs are used when the DOD Personnel Security System of Record is not available.

While there is no standardized format for a VAL, the NISPOM requires it to contain six elements. Generally, the letter identifies the visitor's company information, CAGE Code (if applicable), and certification of the level of the FCL, the visitor's identifying information, PCL information with any special accesses, name of person who is being visited, the purpose and justification for the visit to allow a determination of necessity for the visit, and the date or length of time the VAL is valid.

Since the VAL contains personally identifiable information (PII), it is usually sent to the host organization via fax or encrypted email. Once received, the host is responsible for positively identifying the visitor in the DOD Personnel Security System of Record, determining there is a need-to-know, approving or denying the visit, and ensuring the visitor is only afforded access to classified information consistent with the purpose of the visit.

FCL: Facility Clearance: A Facility Clearance (FCL) is an administrative determination that, from a national security standpoint, a facility is eligible for access to classified information at the same or lower classification category as the clearance being granted. The FCL may be granted at the Confidential, Secret, or Top Secret level.
PCL: Personnel Security Clearance
DOD Personnel Security System of Record: System of record for personnel security, suitability and credential management of all DOD employees, military personnel, civilians, and contractors.

Required Elements of a VAL

Whether a visit involves one or many individuals, all six elements of the visit authorization letter must be presented for each cleared employee. First, the letter must state the requesting contractor's name, address, phone number, CAGE Code, if applicable, and certification of the level of the favorable entity eligibility determination (also referred to as a Facility Clearance, or FCL).

Next, the VAL must provide the name, date and place of birth, as well as citizenship of the employee intending to visit. The third requirement is to specify the proposed visitor's PCL and any special accesses required for the visit. The next element is the name of the person, or persons, to be visited, and the letter must address the necessity for the visit, stating its purpose and justification.

Finally, the letter must indicate the date or period during which the visit authorization letter is to be valid.

VAL: Visit Authorization Letter
CAGE Code - Commercial and Government Entity Code: a five position code that identifies contractors doing business with the Federal Government, NATO member nations, and other foreign governments and is used to support a variety of mechanized systems throughout the government and provides for a standardized method of identifying a given facility at a specific location
FCL: Facility Clearance
PCL: Personnel Security Clearance
NATO: North Atlantic Treaty Organization
CNWDI: Critical Nuclear Weapon Design Information
COMSEC: Communications Security

VAL Transmission

A VAL may be sent via U.S. Postal mail or overnight mail, via a non-electronic means, fax, or via email. In cases of genuine emergencies, a telephone request for authorization can be made. However, it must be immediately followed with a written request in order to obtain an approval signature from the host organization. Under no circumstances, however, should employees hand-carry their personal VALs to the host facility. This would not allow sufficient time for the host organization to verify required information for the visit.

How to send a VAL:

- Electronic transmission
  - Fax
  - Email

When using electronic means, access to the program must be controlled through physical or software protection and have digital signature authentication.

Note: Under NO Under no circumstances should employees be permitted to “hand-carry” their personal VALs to the host facility.

Organization Roles

Visitor’s Organization

When sending an individual on a classified visit at another facility, the visitor’s organization and the host organization has several responsibilities. In keeping with the NISPOM’s requirement to keep the number of visits to a minimum, the visitor’s organization must first determine the need for the visit. The need for access may be outlined in the DD Form 254, but it may also be determined based on an assessment from the host organization. In other words, will the visitor require access to classified information? Or might the visitor come in contact with classified information? And, is the visit in support of a specific classified contract, project, or program that justifies the visit? The FSO can electronically complete and

send the VAL to the host organization. If there is a change in the employee's PCL eligibility or a status change in the visitor company's FCL, the FSO must report those changes.

Note: Communicate employee status/eligibility change or FCL changes.

Host Organization

Once the host organization receives the visit request, the FSO at the host site must review the request. The FSO determines the need for the visit by examining the purpose and justification statements. The FSO may need to talk with the person within the facility that will host the visitor and perhaps the project manager or other subject-matter expert to determine if it is in the interest of the government to approve this classified visit. He or she then confirms the PCL and need-to-know.

If the visitor meets the criteria for an authorized person, the FSO approves the visit request. Approval of the visit request constitutes authority for disclosure of classified information. If there is not a contractual relationship, the host organization must obtain authorization to disclose the classified information from the government contracting activity, or GCA, and must confirm the FCL of the visitor's organization.

Review Activities

Check your answers in the Answer Key in Appendix A of this Student Guide.

Review Activity 1

For each responsibility, identify whether it belongs to the visitor organization, the host organization, or both. *Select all that apply.*

1 of 6. Approve visit or deny visit
- ☐ Visitor's Organization
- ☐ Host Organization

2 of 6. Ensure positive identification of visitor's appropriate PCL: Personnel Security Clearance
- ☐ Visitor's Organization
- ☐ Host Organization

3 of 6. Determine need for classified visit
- ☐ Visitor's Organization
- ☐ Host Organization

4 of 6. Determine need-to-know
- ☐ Visitor's Organization
- ☐ Host Organization

5 of 6. Control visitor's access during visit
- ☐ Visitor's Organization
- ☐ Host Organization

6 of 6. Send visit authorization letter (VAL)
- ☐ Visitor's Organization
- ☐ Host Organization

Review Activity 2

Which of the following are actions the host organization must perform for classified visits in the NISP? *Select all that apply.*

- ☐ Provide disclosure authorization
- ☐ Determine the need for the visit
- ☐ Ensure positive identification of visitors
- ☐ Confirm visitors have appropriate PCL
- ☐ Approve/deny visit request

Lesson 4: Security Controls during Visits

Introduction

During classified visits, visitors must follow the host organization's security controls. The National Industrial Security Program Operating Manual, or NISPOM, requires contractors to establish procedures to ensure that visitors are afforded access only to classified information consistent with the purpose of the visit. In this lesson, you will examine the requirements for security controls in the NISP, as well as some best practices for maintaining security control when hosting a visitor.

Objectives

Here are the lesson objectives.

- Describe how to verify a visitor's identity and access
- Identify security briefing topics for visitors
- Recognize access controls appropriate for a classified visit
- Identify procedures for recovering classified material after a visit
- List best practices for maintaining security control during visits

Security Controls in the NISP

Host Organization Responsibilities

The host organization has several key responsibilities during a classified visit. First, the host organization must verify the visitor's Personnel Security Clearance, or PCL, and need-to-know based on information found in the Visit Authorization Letter, or VAL, or in the DOD Personnel Security System of Record. Then, each visitor's identity must be verified. Acceptable identification must contain both the person's name and photo, such as a driver's license or company photo identification card. The host organization should also brief the visitor on their security procedures as they relate to the classified visit. During the visit, the host must control the activities of visitors to ensure they do not gain access to classified information other than that which is authorized. Finally, the host organization must have procedures in place to recover all classified material.

NISPOM: National Industrial Security Program Operating Manual

Visitors must follow the host organization's security control procedures!

Security Briefings

It is a good security practice for the host organization to review the security procedures a visitor will be expected to follow. This security briefing typically addresses the facility's badging and escort policy, as well as physical security procedures and access areas. It will also discuss use of Portable Electronic Devices, or PEDs, such as cell phones, tablets,

laptops, video and audio recording and playback devices, and receive-only radios.

The briefing may also address how to verify another person's PCL and need-to-know at the host facility prior to a classified discussion.

The briefing should also review how to handle classified documents, such as procedures and equipment for accessing and photocopying, as well as storage. It should explain the policy and procedures for transmitting and/or transporting classified material. This is especially relevant to long-term visitors who are typically working on-site at the host facility to work on a contract. Finally, the security briefing may cover the reporting requirements for security violations, such as loss or compromise of classified material.

When the visit authorization request is sent using the DOD Personnel Security System of Record, if the visit is a first-time visit and the visitor does not have an SF 312, Classified Information Nondisclosure Agreement, in the system, then the host must coordinate with the visitor's security office.

This coordination is to ensure that the SF 312 is signed by the individual and entered into the DOD Personnel Security System of Record prior to the visitor being granted access to classified information. It is a good security practice for the host facility to keep a record of any training provided to visitors.

PED: Portable electronic device
PCL: Personnel Security Clearance
SF 312: Classified Information Nondisclosure Agreement

TIP – Keep a record of training provided to visitors.

Visitor Access Controls

The host must control the activities of visitors so they have access only to classified information consistent with the authorized purpose of the visit. Controlling a visitor's activities prevents unauthorized persons from accessing classified material or overhearing classified discussions for which they are not cleared and do not have a need-to-know.

PCL: Personnel Security Clearance
NISPOM: National Industrial Security Program Operating Manual

Recovery of Classified Material

The final security control in the NISP is the recovery of all classified information when the purpose of the visit has been accomplished or, for visits of more than one day, at the close of each business day. Your end-of-day security check procedures are critical to ensuring that classified material has been properly stored and that the security container has been secured.

Best Practices

In addition to the policy requirements for hosting visitors, there are some best practices that will help your organization maintain security control over the classified information in its possession. One such best practice is to require visitors to sign a visitor record or log. The sign-in sheet may ask for the visitor's name, name of the activity represented, and date of the visit. Although this is not a requirement, it will benefit you for future tracking should an investigation ensue due to an unauthorized disclosure or other security violation.

It is also a good security practice to provide visitors with a badge and an escort when in areas where classified information may be subject to unauthorized disclosure. When needed, the escort must be an appropriately cleared employee who has been informed of the access limitations or restrictions on the visitor's movements. Other best practices include using a card access system, and having clear policies on sanitizing the work area.

Review Activities

Check your answers in the Answer Key in Appendix A of this Student Guide.

Review Activity 1

Which of the following describes how to verify a visitor's identity and access? *Select the best response.*

- ○ Log onto the Facility Clearance System of Record and verify the visitor's Personnel Security Clearance (PCL) and need-to-know
- ○ Verify the visitor's PCL, and need-to-know found in the visit authorization letter (VAL), or in the DOD Personnel Security System of Record, and then verify the visitor's name and photo identification before giving the person access.
- ○ Verify the visitor's name and photo identification in the Facility Clearance System of Record

Review Activity 2

List the five security control requirements when hosting a classified visit discussed in this lesson.

1.
2.
3.
4.

Review Activity 3

Which of the following may be topics of the security briefing for visitors? *Select all that apply.*

- ☐ Badging and escort policy
- ☐ Physical security procedures and access areas
- ☐ Use of Portable Electronic Devices
- ☐ How to handle classified documents, such as procedures and equipment for accessing and photocopying, as well as storage
- ☐ Policy and procedures for transmitting and/or transporting classified material
- ☐ Reporting requirements for security violations
- ☐ How to verify another person's PCL and need-to-know at the host facility prior to a classified discussion

Review Activity 4

Which of the following are access controls appropriate for a classified visit? *Select all that apply.*

- ☐ Control visitor activities so they have access only to classified information consistent with the authorized purpose of the visit
- ☐ Prevent the visitor from accessing classified information in the secure storage cabinet
- ☐ Ensure unauthorized persons cannot overhear classified discussions for which they are not cleared and do not have a need-to-know

Review Activity 5

When the purpose of the visit has been accomplished, or at the close of each day, what's the final security control? *Select the best response.*

- ○ Ensure the classified documents have the proper cover page and are placed in a desk file folder for work/use the next day.
- ○ Recover all classified and store/secure in security container or approved area.
- ○ Verify documents have not been altered before they leave the facility.

Review Activity 6

Which of the following are best practices for maintaining security control over classified information? *Select all that apply.*

- ☐ Require visitors to sign a visitor record or log.
- ☐ Provide visitors with a badge and an escort when in areas where classified information may be subject to unauthorized disclosure.
- ☐ Use a card access system.
- ☐ Have clear policies on sanitizing the work area.

Lesson 5: International and NATO Visits

Introduction

Industry and government workers may have to support contracts requiring visits abroad or hosting foreign visitors in the U.S. This lesson will examine the international security requirements for international and NATO visits as outlined in the National Industrial Security Program Operating Manual, or NISPOM, and Department of Defense Directive 5230.20, Visits and Assignments of Foreign Nationals. The lesson will explore the approval process for incoming and outgoing visitors and required security controls.

Objectives

Here are the lesson objectives.

- Identify the requirements and security controls for incoming and outgoing international visits
- Describe the process for international visit approval including the role of the contractor, embassy, and Foreign Visits System (FVS)
- Identify the requirements and security controls for NATO visits

NISPOM: National Industrial Security Program Operating Manual
NATO: North Atlantic Treaty Organization.

NISP International Visit Policy

International Visits Overview

As you learn about the NISP international visit policies, there are three key visit relationships this lesson will address: visits by foreign nationals or representatives of a foreign government to U.S. contractor facilities, visits abroad by U.S. contractors, and North American Treaty Organization or NATO related visits.

Visits by foreign nationals or representatives of a foreign government to U.S. contractor facilities are called incoming international visits.

Visits abroad by U.S. contractors are referred to as outgoing international visits. NATO related visits include all visits involving a NATO Command or Agency or the NATO International Staff, including U.S. citizens assigned to NATO, that involve access to NATO Information or U.S. classified information.

Each of these three visit categories have different requirements and approval processes. However, they do share two requirements.

All international visits require submission of a visit request and all require an export authorization before disclosing to a foreign person any classified information or Controlled Unclassified Information, or CUI. This lesson will discuss each category and outline the applicable requirements and procedures.

Export authorization: An approved numbered license or agreement or an authorized exemption under the ITAR. Written approval by a GCA of a visit request is considered to be the export authorization if the approval clearly identifies the information that will be disclosed.
NATO: North Atlantic Treaty Organization

Visit Duration

International visits can take place over different time periods. The NISPOM details some of these differences. One-time visits are for a single, short-term occasion for a specified purpose. These visits normally last less than 30 days.

Recurring visits are intermittent over a specified period of time in support of a government-approved arrangement, such as a program or contract. Normally recurring visits may last for up to one year. The governments agree to the authorization terms, which are subject to annual review and validation.

The third type of international visit is an extended or long-term visit. This is a single visit for an extended period of time, normally up to 1 year, in support of a government-approved agreement or contract. An extended visit authorization must be reviewed annually to ensure there is a continued requirement for the international visitor to remain at the site and the information in the visit authorization is current.

Sometimes emergencies arise that require an international visit. Emergency visits may be approved only as a single one-time visit.

Government-approved arrangement: A Government-approved arrangement may be an agreement, contract,or export license.
NISPOM: National Industrial Security Program Operating Manual

Emergency Visit

To qualify as an emergency visit, the visit must relate to a specific Government-approved contract, international agreement, or announced request for proposal. Requests will be approved for a single, one-time visit only. An additional qualification is that failure to make the visit could be reasonably expected to seriously jeopardize performance on the contract or program, or result in the loss of a contract opportunity. The requester must submit an emergency visit request and should coordinate with a knowledgeable person at the government agency which is the Government Contracting Activity, or GCA, of the industrial facility to be visited to ensure the emergency visit request has all the necessary details.

RE: Emergency Visit

Visit authorizations shall not be used to employ or otherwise acquire the services of foreign nationals that require access to export-controlled information. An export authorization is required for such situations.

Emergency Letter of Justification Requirements:

- Justification letter must be on Government Contracting Agency (GCA) or foreign official letterhead and signed by the GCA or foreign site to be visited. Emails are acceptable, permitted they have the official signature block from the GCA program manager or foreign site POC.
- State the reason for the emergency visit and express why it cannot be rescheduled for a later date.
- The letter of justification should be specific to the visit (visitors, company name, program/project).
- Identify the beginning and ending dates of visit.
- Agendas or Letter of Invitations are not considered an emergency justification letter.

Incoming International Visits

Governing Rules

Incoming visits by foreign nationals or foreign government representatives are subject to two separate regulatory frameworks.

One framework is policy on disclosing classified national security information to foreign entities. Contractors must follow the provisions of the NISPOM, while DOD personnel must follow DOD Directive 5230.20 on visits and assignment of foreign nationals.

The other regulatory framework that governs incoming visits is U.S. export control policy. The International Traffic in Arms Regulations, or ITAR, sets forth the rules and procedures with respect to export of defense articles and defense services. This includes export of both classified and unclassified information.

These two frameworks, however, use different definitions for what constitutes a foreign entity. For example, the NISPOM defines a foreign national as any person who is not a U.S. citizen or national. This definition does not include foreign businesses. The NISPOM defines a foreign interest, however, to include foreign businesses, as well as foreign governments or their representatives.

The ITAR uses only one term: foreign person. This term is different from the NISPOM because it does not include all non-U.S. citizens. Certain non-U.S. citizens – eligible for protection under U.S. immigration law – are not considered foreign persons under the ITAR. The ITAR definition of foreign person also includes foreign government entities and business structures. For this reason, it is important to refer to the specific definition in the policy document with which you are seeking to comply.

NISPOM: National Industrial Security Program Operating Manual
DODD: Department of Defense Directive
Foreign national: In accordance with the NISPOM, any person who is not a citizen or national of the United States.
Foreign interest: Any foreign government, agency of a foreign government, or representative of a

foreign government; any form of business enterprise or legal entity organized, chartered or incorporated under the laws of any country other than the United States or its territories, and any person who is not a citizen or national of the United States.
Foreign person: Foreign person means any natural person who is not a protected individual as defined by 8 U.S.C. 1324b(a)(3). It also means any foreign corporation, business association, partnership, trust, society or any other entity or group that is not incorporated or organized to do business in the United States, as well as international organizations, foreign governments and any agency or subdivision of foreign governments (e.g., diplomatic missions). (ITAR)

Visit Procedures and Requirements

Incoming international visits require the sponsoring foreign government to submit a Request For Visit, or RFV, through government channels. The cognizant U.S. Government agency will then approve or reject the RFV. If the U.S. approves a visit, it issues a notification of approval detailing the level and scope of classified and unclassified information authorized for disclosure, as well as any limitations.

Contractors must establish procedures to monitor incoming international visits or to ensure that the disclosure of and access to export-controlled articles and related information are limited to those that are approved by an export authorization. For long-term foreign visitors or employees, contractors should document procedures in a Technology Control Plan, or TCP.

In the event the Government does not approve the incoming international visit, different requirements apply.

Limitations

U.S. agency approval notification details clearance level/limitations:

- Visit requests approved by the DOD constitute an exemption to the export licensing provisions of Part 125.5 of the ITAR when the technical data authorized for disclosure is **fully described**
- If the technical data is **not** fully described, the contractor to be visited must obtain an export license

Export Authorization:

- Visit authorizations shall not be used to employ or otherwise acquire the services of foreign nationals that require access to export-controlled information. An export authorization is required for such situations.
- In cases of commercial programs and related unclassified information, it is the contractor's responsibility to ensure that an export authorization is obtained, if applicable.

TCP: Technology Control Plan
RFV: Request for Visit.

RFV Rejection

When visit requests by foreign nationals are not in support of a U.S. Government program, the government will render a declination notice. This means that the visit does not have government sponsorship.

The declination notice is sent to both the requesting foreign government and to the U.S. contractor to be visited. The visit may still proceed, but the contractor must have, or obtain, an export authorization for the information involved. This would normally be in the form of an export license issued by the Department of State, Directorate of Defense Trade Controls, or the Department of Commerce.

Additionally, if classified information is involved, the contractor must ensure the requesting foreign government has provided the required security assurance of the proposed visitor to the U.S. Government agency in the original visit request. The contractor must also determine licensing requirements regarding the disclosure of export-controlled information during the visit.

NISPOM: National Industrial Security Program Operating Manual
Security assurance: A statement that the individual meets eligibility requirements for access to classified information

Approval Process

The DOD International Visits Program, or IVP, is used to process visits and assignments of foreign nationals to the DOD Components and cleared contractor facilities. There are two ways in which requests for visits by foreign nationals within the U.S. are processed. The RFV may be submitted through the sponsoring government's embassy in Washington, D.C. or by the sponsoring organization using the automated Foreign Visits System, or FVS, and IVP procedures. The foreign government is also required to submit a written confirmation of security assurance that the visitor(s) is properly cleared, has a need-to-know, and will comply withany security requirements specified by the United States.

Requests for visits by foreign nationals that involve only commercial programs and related unclassified information are submitted directly to the contractor.

RFV: Request for Visit
IVP: International Visits Program (IVP): Is designed to ensure that classified information and CUI to be disclosed to such visitors has been properly authorized for disclosure to their governments, to ensure that the requesting foreign government provides a Security Assurance for the proposed visitor when classified information is involved in the visit or assignment, and to facilitate administrative arrangements (e.g., date, time, and place) for the visit or assignment.
FVS: Foreign Visits System (FVS): The automated system operated by the Office of the USD(P) that provides staffing and database support for processing RFVs by foreign nationals to DOD Component activities and defense contractors.
Security assurance: A written confirmation by a responsible foreign government official that the proposed visitor possesses the requisite security clearance and need-to-know for the classified information and CUI to be released during the visit. The Security Assurance certifies that the

recipient government will protect the information in accordance with the international agreement between the U.S. and the foreign government.

Security Controls During Foreign Visits

Security Controls

Security controls for international visits are required to protect the nation's sensitive information. Contractors must maintain a record of foreign visitors for one year when the visit involves access to classified information. In most cases, the visit authorization constitutes an export authorization. Therefore, the records must be maintained for five years in compliance with the ITAR.

As more U.S. contractor facilities become involved with foreign entities, some companies have reported incidents involving foreign visitors attempting to gain unauthorized access to classified or export-controlled information.

To mitigate these threats it is important to implement security countermeasures, which should be included in the required technology control plan, or TCP. A TCP stipulates how a company will control access to its export-controlled technology and outlines the specific information that has been authorized for release.

If your facility encounters any suspicious contact, it should be reported to your Defense Counterintelligence and Security Agency Industrial Security Representative, or IS Rep. Reports of actual, probable, or possible espionage, sabotage, terrorism, or subversive activities should be reported to the FBI with a copy to the DCSA IS Rep.

NISPOM: National Industrial Security Program Operating Manual
TCP: Technology Control Plan.

Security Countermeasures

- Develop and implement a Technology Control Plan (TCP)
- Employees should be knowledgeable of the company’s Empowered Official, who is responsible for all export control issues.
- Conduct frequent computer security audits
- Contract terms specify that all communication to & from the facility must be in English
- Do not respond to requests for visas which may be an attempt to circumvent export controls
- Should be appropriate to counter specific threats

Empowered Official
ITAR defines an Empowered Official as a U.S. person:

- Employed by the applicant/subsidiary with authority for policy or management
- Legally empowered to sign license applications or requests on behalf of the applicant
- Understands the requirements of export control statutes and penalties for violating the

AECA and ITAR

- Authorized to:
  - Enquire into a proposed export, temporary import, or brokering activity
  - Verify legality and accuracy
- Refuse to sign any license application or other request

Specific threats: Counterintelligence organizations can help identify specific threats. FSOs should seek information from the DCSA Counterintelligence (CI) office and from the GCA.

Technology Control Plan (TCP)

Purpose:

- Protect classified and export-controlled information
- Control access by long-term foreign visitors
- Control access by employees who are foreign persons

The TCP must:

- Identify responsible company officials
- Contain procedures to control access
- Provide disclosure guidelines to all export-controlled information
- Provide for indoctrination and security training for all company employees
- Designate a monitor to oversee implementation of the plan
- Be tailored to company operations

Extended Visits

Extended visits and assignment of foreign nationals to contractor facilities are authorized only when it is essential to a contract or agreement, such as a joint venture or multinational program. In advance of the visit, the contractor must: obtain written consent of the GCA, if export-controlled information is required; submit a request for export authorization, if needed; and notify the CSA of all extended visits and assignments of foreign nationals to its facility. The notification needs to include a copy of the approved visit authorization or the U.S. Government export authorization, and the TCP.

GCA: U.S. Government Contracting Activity
CSA: Cognizant Security Agency
RFV: Request for Visit.

Outgoing International Visits

Visit Requirements

The NISPOM provides guidance on visits abroad by U.S. contractors, or outgoing visits. International visits must meet the NISPOM requirements when: the information is either classified information; or is unclassified information that is either related to classified contracts, or is subject to export controls under the ITAR or EAR.

When contractor employees visit foreign government facilities or foreign contractors on U.S. Government orders in support of a government contract or agreement, contractors must submit a visit request through government channels. Many foreign governments require the submission of a visit request for all visits to a government facility or a cleared contractor facility, even though classified information may not be involved. The visit request must be forwarded through government channels to the security official designated by the Cognizant Security Agency, or CSA. An export authorization or disclosure decision must be obtained for any classified or unclassified controlled information to be disclosed during the visit. If the disclosure is covered by an ITAR exemption, however, export authorization is not required.

RFV: Request for Visit
CSA: Cognizant Security Agency (CSA): Agencies of the Executive Branch that have been authorized by E.O. 12829 to establish an industrial security program for the purpose of safeguarding classified information under the jurisdiction of those agencies when disclosed or released to U.S. Industry. Department of Defense, the Department of Energy, the Central Intelligence Agency, and the Nuclear Regulatory Commission. When the DOD is the CSA, international visits are facilitated by DCSA Headquarters.
ITAR: International Traffic in Arms Regulations (ITAR): Control the export and import of defense-related articles and services on the U.S. Munitions List (defense and military-related technologies).
EAR: Export Administration Regulations
NISPOM: National Industrial Security Program Operating Manual

Approval Process

Requests for outgoing visits, also known as RFV Form U-1201, must be faxed to the DCSA Headquarters. DCSA Headquarters verifies the proposed visitor's clearance and transmits the request to the U.S. Embassy in the foreign country to be visited.

The Embassy office processes and forwards the visit request to the appropriate foreign government office, which is usually the country's Ministry of Defense. If the foreign government office approves the visit, the approval is forwarded to the site to be visited.

If the foreign government rejects the visit request, DCSA Headquarters is the entity that communicates this back to the contractor. The visitor organization is responsible for ensuring that the host organization coordinates with the government authorities required to approve the visit. Countries vary in the amount of advance notice they require before a visit. It can take anywhere from 15 to 40 days to approve an RFV.

RFV: Request for Visit

NATO Visits

Overview of NATO-Related Visits

In order for a contractor to negotiate or perform on a NATO classified contract, it must have a NATO Facility Security Clearance Certificate, or FSCC. The DOD Cognizant Security Agency (CSA) office will provide the required NATO certification of security clearance to the NATO Security Authorities. In order for an individual to access NATO classified information, he or she must have a final personnel clearance, or PCL, at the equivalent level and must have received a NATO Briefing and signed a NATO Briefing Certificate.

NATO Classification Levels

NATO has the following levels of security classification:

- COSMIC TOP SECRET (CTS)
- NATO SECRET (NS)
- NATO CONFIDENTIAL (NC)
- NATO RESTRICTED (NR)
- ATOMAL information is marked:
  - COSMIC TOP SECRET ATOMAL (CTSA)
  - NATO SECRET ATOMAL (NSA)
  - NATO CONFIDENTIAL ATOMAL (NCA)
- ATOMAL applies to:
  - U.S. RESTRICTED DATA or FORMERLY RESTRICTED DATA
  - United Kingdom Atomic information released to NATO

FSCC: Facility Security Clearance Certificate
CSA: Cognizant Security Agency
PCL: Personnel Security Clearance
NISPOM: National Industrial Security Program Operating Manual

Approval Process

The NATO visit approval process is slightly simpler than for international outgoing visits. The request to visit a NATO site is still processed through DCSA Headquarters. The difference is that DCSA Headquarters sends the approval directly to the NATO site.

Security Controls

Contractors are required to maintain a separate record of NATO visits, including those by U.S. personnel assigned to NATO. In accordance with the NISPOM, these records must be kept for three years. Employees must be given an initial NATO security briefing covering topics on access, preparing and marking NATO documents, storage, distribution, handcarrying, and reproduction. Release of U.S. classified or export-controlled information to NATO requires an export authorization or other written disclosure authorization. In accordance with the ITAR, these records must be maintained for five years.

NISPOM: National Industrial Security Program Operating Manual

NATO Briefings include:

- Access, preparing and marking NATO documents, storage, distribution, hand carrying, reproduction
- Annual refresher and debriefing:
  - Signed certificate required

Review Activities

Check your answers in the Answer Key in Appendix A of this Student Guide.

Review Activity 1

Which of the following are host organization requirements and security controls for an incoming international visit? *Select all that apply.*

- ☐ Obtain an export authorization for discussion of classified information.
- ☐ Prepare a Technology Control Plan (TCP) for long-term visitors.
- ☐ Implement access controls to limit disclosure to export authorization.
- ☐ Maintain a visitor record

Review Activity 2

Which of the following are the steps for an outgoing international visit? *Select the steps of the outgoing international visit approval process.*

- ☐ The U.S. contractor submits a Request for Visit (RFV) through the Foreign Visits System (FVS).
- ☐ The U.S. contractor faxes the RFV to DCSA Headquarters.
- ☐ The RFV is forwarded by DCSA Headquarters to the U.S. Embassy in the foreign country to be visited.
- ☐ The U.S. Embassy forwards the approved RFV to the visit site.
- ☐ The U.S. Embassy forwards the RFV to the foreign government office for approval.
- ☐ The foreign government office sends the approved RFV to the visit site.

Review Activity 3

A foreign national is being assigned to work with your company and requires extended visit approval. *Select all the steps of the incoming international visit approval process.*

- ☐ The foreign government office may submit a Request for Visit (RFV) through the Foreign Visits System (FVS).
- ☐ The foreign government office may submit an RFV to the DCSA Headquarters.
- ☐ The foreign government office may submit an RFV to its embassy in Washington, D.C.
- ☐ The foreign government office submits a written confirmation of security assurance.
- ☐ Once the RFV is approved, DCSA Headquarters notifies the U.S. contractor.

Review Activity 4

Which of the following are requirements and security controls for NATO visits involving classified information at a U.S. facility? *Select all that apply.*

- ☐ Obtain written consent of NATO member's government
- ☐ Maintain visitor records for three (3) years
- ☐ Provide a declination notice to the foreign government
- ☐ Annual security briefings and exit debrief with signed certificate
- ☐ Export authorization
- ☐ Obtain a Facility Security Clearance Certificate (FSCC) from the CSA

Lesson 6: Classified Meetings

Introduction

Classified meetings are sponsored by the Government Contracting Activity, or GCA. Meetings are gatherings of many people, often representing many different government organizations and cleared contractor facilities, at a conference, seminar, symposium, exhibit, convention, training course, or other gathering during which classified information is disclosed. Classified meetings have different procedural requirements that visitor and host organizations must follow when disclosing classified information. This lesson will examine the responsibilities of the GCA in sponsoring classified meetings, and will look at the steps involved for a contractor to hold a classified meeting.

Objectives

Here are the lesson objectives.

- Recognize responsibilities of the Government Contracting Activity (GCA) in sponsoring classified meetings
- Indicate steps involved for a contractor to host GCA-sponsored meetings
- Identify security control responsibilities for hosting a classified meeting

To be a **classified meeting** under the NISPOM, the gathering must be sponsored by a government agency to serve a government purpose.

NISPOM: National Industrial Security Program Operating Manual

Meetings Overview

Government Sponsorship

Classified meetings are sponsored by a government agency to serve a government purpose. Cleared contractors can host these meetings provided a government agency has authorized it and assumes security jurisdiction. However, disclosure of classified information to large diverse audiences increases security risks. This lesson will examine requirements designed to help mitigate these risks.

Responsibilities of the GCA

The GCA must approve security arrangements, announcements, attendees, and the location of the meeting. Some duties may be delegated to the contractor provided the GCA maintains supervision. The GCA security officer is responsible for verifying attendees' Personnel Security Clearances, or PCLs, as well as their justification for attendance in the DOD Personnel Security System of Record.

Additionally, all persons attending classified sessions must have a need-to-know for the information to be disclosed. Need-to-know may be determined by the authorizing agency or

its designee based on the justification provided. Finally, the GCA must approve the location for the meeting.

PCL: Personnel Security Clearance
NISPOM: National Industrial Security Program Operating Manual

Requests to Attend Classified Meetings

Before a contractor employee can attend a classified meeting, the contractor shall provide justification

- Why the employee requires access to the classified information,
- Cite the classified contract or GCA program/project involved, and
- Forward the information to the authorizing government agency.

Holding a Classified Meeting

Request for Authorization

Cleared contractors often will host GCA-sponsored meetings. In order to do so, they must first submit a request for authorization to the government agency that has agreed to assume security jurisdiction. The request should contain an explanation of the government purpose and why conventional channels for release of the classified information will not advance those interests.

The request also includes the specifics on the subject, scope, security classification levels, security arrangements, dates and location, and attendees. The attendees listed should include any non-government organization involved including a full description of the type of support it will provide. Also listed should be any proposed foreign representatives, including their nationality, name and organizational affiliation.

Announcements

If a cleared contractor's request to host a classified meeting is granted, it will then issue anannouncement or invitation. It may contain only unclassified information limited to general descriptions and speaker names. Announcements can also provide administrative instructions and general statements on what the government agency has authorized to provide, such as those listed here. Invitations to foreign visitors are issued by the authorizing government agency, not thehosting contractor.

Announcements/Invitations

State only that the government agency:

- Has authorized the conduct of classified sessions
- Will provide necessary security assistance
- Forward to the authorizing agency or its designee, the participant's:
  - Security clearances

- Justification to attend

Invitations to foreign persons shall be sent by the authorizing government agency.

Meeting Location

Classified sessions may be held only at a Federal Government installation or a cleared contractor facility. The GCA must verify the company's Facility Clearance, or FCL, level and safeguarding capability through the FCL System of Record. Once the FCL and safeguarding verification is made, the GCA must approve all physical security and procedural security controls before authorizing the meeting.

GCA: Government Contracting Activity
FCL: Facility Clearance: An administrative determination that, from a national security standpoint, a facility is eligible for access to classified information at the same or lower classification category as the clearance being granted. The FCL may be granted at the Confidential, Secret, or Top Secret level.
FCL System of Record: The electronic system that all companies must use while in process for an FCL or to report a changed condition. It is also a repository of information about DOD cleared contractor facilities. The system has internal users (with full access such as DCSA personnel) and external users (with limited access).

Security Controls

Responsibilities of Participants and Attendees

Once the GCA approves a meeting, measures must be implemented for security control of the participants. First, each organization planning to share classified information must obtain prior written authorization to do so. This authorization comes from the government agency with jurisdiction over the information involved and a copy must be furnished to the government agency sponsoring the meeting.

Meeting attendees must present official identification such as a passport or U.S. Government ID card to gain entry into the session. Presentations must contain appropriate classification guidance so that attendees know what information is classified and the level of classification. Presentations must be delivered orally and/or visually.

Copies of classified presentations cannot be distributed at the meeting and any classified notes or electronic recordings must be appropriately marked, safeguarded, and transmitted as required by the NISPOM.

Disclosure Authority at Meetings

A contractor desiring to disclose classified information at a meeting shall:

a. Obtain prior written authorization for each proposed disclosure of classified information from the government agency having jurisdiction over the information involved.

b. Furnish a copy of the disclosure authorization to the government agency sponsoring the meeting.

c. Associations are not responsible for ensuring that classified presentations and papers of other organizations have been approved for disclosure. Authority to disclose classified information at meetings, whether disclosure is by officials of industry or government, must be granted by the government agency or activity that has classification jurisdiction over the information to be disclosed. Each contractor that desires to disclose classified information at a meeting is responsible for requesting and obtaining disclosure approvals.

NISPOM: National Industrial Security Program Operating Manual

Responsibilities of Host

Once the attendees have been cleared and determined to have a need-to-know, the host organization must put their names on an access list to the classified session. Although the host organization is responsible for physical security measures during classified sessions, they must be approved by the GCA. These measures must provide for control of, access to, and dissemination of, the classified information to be presented, and provide for secure storage capability, if necessary.

If necessary, the host organization must also provide secure storage capability for classified documents. Host organizations must ensure any classified notes or electronic recordings of classified presentations shall be appropriately marked, safeguarded, and transmitted according to the NISPOM.

Host organization security control responsibilities:

- Prepare a list of authorized attendees
- Provide physical security controls for:
    - Control, access and dissemination of classified information
    - Secure storage, if necessary
    - Consult the TCP, if applicable
- Ensure notes and recordings are appropriately marked, safeguarded, and transmitted according to the NISPOM

Review Activities

Check your answers in the Answer Key in Appendix A of this Student Guide.

Review Activity 1

For each listed procedure or security control, identify which entity is responsible. *Make your selection.*

1 of 5. Verify Personnel Security Clearance (PCL) and need-to-know
- ☐ Government Contracting Activity (GCA)
- ☐ Hosting Organization
- ☐ Participant / Presenter

2 of 5. Verify Facility Clearance (FCL)
- ☐ Government Contracting Activity (GCA)
- ☐ Hosting Organization
- ☐ Participant / Presenter

3 of 5. Provide security classification guidance on information presented
- ☐ Government Contracting Activity (GCA)
- ☐ Hosting Organization
- ☐ Participant / Presenter

4 of 5. Collect, safeguard, and transmit classified notes or recordings
- ☐ Government Contracting Activity (GCA)
- ☐ Hosting Organization
- ☐ Participant / Presenter

5 of 5. Obtain authorization for disclosure of classified information from the agency with jurisdiction over it
- ☐ Government Contracting Activity (GCA)
- ☐ Hosting Organization
- ☐ Participant / Presenter

Review Activity 2

Which of the following are responsibilities of the Government Contracting Activity (GCA) in sponsoring contractor proposed classified meetings? *Select all that apply.*

- ☐ Ensure the meeting serves a government purpose
- ☐ Provide a declination notice to the foreign government
- ☐ Process the contractor's request for authorization
- ☐ Ensure adequate security measures are provided in advance, including announcements, requisite participant clearance and need-to-know, and compliance with presentation material requirements, and physical security measures are in place
- ☐ Evaluate and approve the proposed location
- ☐ Ensure the announcement specifies the security clearances, justification to attend, and topics to be discussed in classified sessions

Review Activity 3

Which of the following are steps involved for a contractor to host GCA-sponsored meetings? *Select all that apply.*

- ☐ Submit a request for authorization to the government agency that has agreed to assume security jurisdiction
- ☐ Obtain a Facility Security Clearance Certificate (FSCC) from the CSA
- ☐ Issue an announcement or invitation to non-foreign visitors once the request to host a classified meeting is granted

Review Activity 4

Which of the following are disclosure authority requirements for contractors desiring to disclose classified information at a meeting? *Select all that apply.*

- ☐ Obtain prior written authorization for each proposed disclosure from the government agency having jurisdiction over the information
- ☐ Obtain a Facility Security Clearance Certificate (FSCC) from the CSA
- ☐ Furnish a copy of the disclosure authorization to the government agency sponsoring the meeting

Review Activity 5

Which of the following are security control responsibilities for hosting a classified meeting? S*elect all that apply.*

- ☐ Obtain prior written authorization for each proposed disclosure from the agency with jurisdiction over the information
- ☐ Implement physical security measures approved by the GCA for control of, access to, and dissemination of, the classified information to be presented
- ☐ Provide for secure storage capability, if necessary
- ☐ Ensure security classification guidance on information presented
- ☐ Ensure presentation delivery is oral/visual
- ☐ Distribute classified presentations at the meeting
- ☐ Ensure notes and recordings are appropriately marked, safeguarded, and transmitted according to the NISPOM

Lesson 7: Course Conclusion

Conclusion

Summary

Visits and meetings in the National Industrial Security Program, or NISP, require vigilance to protect the nation's classified information using security measures to mitigate the risk of unauthorized disclosure, while pursuing the government's purpose. You should now know the basic concepts and procedures concerning classified visits and government sponsored meetings as well as the security controls required by both visitor organizations and host organizations. You should also know the sources of guidance to consult for greater detail.

NISPOM: National Industrial Security Program Operating Manual

Lesson Review

Here is a list of the lessons in the course.

- Course Introduction
- Visit Basics
- Procedures for Classified Visits
- Security Controls during Visits
- International and NATO Visits
- Classified Meetings
- Course Conclusion

Course Objectives

You should now be able to perform all of the listed activities. Congratulations. You have completed the *Visits and Meetings in the NISP Course*. To receive course credit, you MUST take the Visits and Meetings in the NISP examination. Follow the instructions on screen to access the online exam.

You should now be able to:

- Identify the requirements for classified visits in the NISP
- Identify the authorization responsibilities and procedures when sending an employee on a classified visit
- Identify the authorization responsibilities and procedures when hosting a classified visit
- Describe how to verify a visitor’s identity and access
- Identify security briefing topics for visitors
- Recognize access controls appropriate for a classified visit
- Identify procedures for recovering classified material after a visit
- List best practices for maintaining security control during visits

- Identify the requirements and security controls for incoming and outgoing international visits
- Describe the process for international visit approval including the role of the contractor, embassy, and Foreign Visits System (FVS)
- Identify the requirements and security controls for NATO visits
- Recognize responsibilities of the Government Contracting Activity (GCA) in sponsoring classified meetings
- Indicate steps involved for a contractor to host GCA-sponsored meetings
- Identify security control responsibilities for hosting a classified meeting

To receive course credit you MUST take the Visits and Meetings in the NISP examination. Please use the STEPP system from the Center for Development of Security Excellence to register for the online exam.

Appendix A: Answer Key—Review Activities

Lesson 2 Review Activities

Review Activity 1

1 of 3: Regardless of the visit duration, all visitors, whether government employees or contractors, must follow the host organization's security procedures.

- ⊙ True *(correct response)*
- ○ False

***Feedback**: Regardless of the visit duration, all visitors, whether government employees or contractors, must follow the host organization's security procedures.*

2 of 3: When a contractor employee visits a government facility, he or she must follow the security requirements of that facility and the visitor's organization is relieved from continued security oversight of that employee.

- ○ True
- ⊙ False *(correct response)*

***Feedback**: Even though a contractor employee must follow the security requirements when visiting a government facility, this does not relieve the visitor's organization from continued security oversight of that employee.*

3 of 3: Government personnel assigned to or visiting a contractor facility and engaged in oversight of an acquisition program do not have to relinquish control of their work products to the contractor.

- ⊙ True *(correct response)*
- ○ False

***Feedback**: Government personnel assigned to or visiting a contractor facility and engaged in oversight of an acquisition program will retain control of their work products.*

Review Activity 2

What are the key requirements for a classified visit in the NISP?

☑ Visits must be held to a minimum. *(correct response)*

☐ The visitor must certify that access is consistent with the purpose of the visit and show positive identification.

☑ The purpose for the visit must be in the national interest and cannot be achieved without access to classified information. *(correct response)*

☑ The contractor must ensure the visitor has a Personnel Security Clearance (PCL) and need-to-know and provides positive identification. *(correct response)*

***Feedback**: Visits must be held to a minimum and must be in the interest of national security. A classified visit is not authorized unless its purpose cannot be achieved without access to classified information. The contractor must ensure the visitor has a PCL and need-to-know and provides positive identification.*

Review Activity 3

The purpose for a classified visit in the NISP is to share classified information for a lawful and authorized U.S. Government purpose.

⦿ True *(correct response)*

○ False

***Feedback**: The purpose for a classified visit in the NISP is to share classified information for a lawful and authorized U.S. Government purpose.*

Review Activity 4

Which of the following are the visitor's authorization requirements for accessing classified information?

☑ The authorized person must have been granted a Personnel Security Clearance (PCL) at the required level. *(correct response)*

☐ The authorized person must have been granted access at a higher level than the host organization's Facility Clearance (FCL).

☐ The person must have a PCL at the required level, but a need-to-know determination is not required unless the information is Top Secret.

☑ The authorized person must have a need-to-know the classified information in the performance of official duties. *(correct response)*

***Feedback**: The authorized person must have been granted a PCL at the required level and have a need-to-know the classified information in the performance of official duties.*

Review Activity 5

Which of the following are responsibilities of a host organization during a classified visit?

- ☑ Determine that the visit is necessary in the interest of national security *(correct response)*
- ☐ Request disclosure authority from the visitor's organization
- ☑ Determine that the purpose of the visit cannot be achieved without access to, or disclosure of, classified information *(correct response)*
- ☑ Ensure that the visitor's identity is confirmed and he or she has the proper PCL and need-to-know *(correct response)*

Feedback*: The host organization's responsibilities include: (1) Determine that the visit is necessary in the interest of national security; (2) Determine that the purpose of the visit cannot be achieved without access to, or disclosure of, classified information; and (3) Ensure that the visitor's identity is confirmed and he or she has the proper PCL and need-to-know.*

Lesson 3 Review Activities

Review Activity 1

For each responsibility, identify whether it belongs to the visitor organization, the host organization, or both.

1 of 6. Approve visit or deny visit

- ☐ Visitor's Organization
- ☑ Host Organization *(correct response)*

***Feedback**: The host organization approves or denies the visit request. Approval of the visit request constitutes authority for disclosure.*

2 of 6. Ensure positive identification of visitor's appropriate PCL (Rollover for PCL: Personnel Security Clearance)

- ☐ Visitor's Organization
- ☑ Host Organization *(correct response)*

***Feedback**: The host organization must ensure positive identification of visitor's appropriate PCL.*

3 of 6. Determine need for classified visit

- ☑ Visitor's Organization
- ☑ Host Organization *(correct response)*

***Feedback**: Both the visitor's organization and the host organization must confirm the need for the classified visit. This ensures the visit is in furtherance of a government contracting activity (GCA) purpose and helps keep the number of visits to a minimum.*

4 of 6. Determine need-to-know

- ☐ Visitor's Organization
- ☑ Host Organization *(correct response)*

***Feedback**: The entity that will disclose classified information must make the "need-to-know" determination. This is usually the host organization.*

5 of 6. Control visitor's access during visit

- ☐ Visitor’s Organization
- ☑ Host Organization *(correct response)*

Feedback*: The host organization is responsible for controlling the visitor’s access. Visitors must always follow the host organization’s security procedures.*

6 of 6. Send visit authorization letter (VAL)

- ☑ Visitor’s Organization
- ☐ Host Organization *(correct response)*

Feedback: *The visitor’s organization sends the visit authorization letter (VAL).*

Review Activity 2

Which of the following are actions the host organization must perform for classified visits in the NISP?

- ☑ Provide disclosure authorization *(correct response)*
- ☑ Determine the need for the visit *(correct response)*
- ☑ Ensure positive identification of visitors *(correct response)*
- ☑ Confirm visitors have appropriate PCL *(correct response)*
- ☑ Approve/deny visit request *(correct response)*

Feedback: *All of these are actions the host organization must perform for visits in the NISP.*

Lesson 4 Review Activities

Review Activity 1

Which of the following describes how to verify a visitor's identity and access?

- ○ Log onto the Facility Clearance System of Record and verify the visitor's Personnel Security Clearance (PCL) and need-to-know
- ⊙ Verify the visitor's PCL, and need-to-know found in the visit authorization letter (VAL), or in the DOD Personnel Security System of Record, and then verify the visitor's name and photo identification before giving the person access *(correct response)*
- ○ Verify the visitor's name and photo identification in the Facility Clearance System of Record

Feedback*: Verify the visitor's PCL, and need-to-know found in the visit authorization letter (VAL), or in the DOD Personnel Security System of Record, and then verify the visitor's name and photo identification before giving the person access.*

Review Activity 2

List the five security control requirements when hosting a classified visit discussed in this lesson. (Screen Question/Instructions: Can you list the five security control requirements when hosting visitors? *Type your answers in the space provided; then select Done.*)

Feedback*: The host organization has key requirements when hosting visitors:*

- *Verify the visitor's Personnel Security Clearance (PCL) and need-to-know*
- *Verify the visitor's identity*
- *Brief the visitor on security procedures*
- *Limit the visitor's access to information*
- *Recover all classified material*

Review Activity 3

Which of the following may be topics of the security briefing for visitors?

- ☑ Badging and escort policy *(correct response)*
- ☑ Physical security procedures and access areas *(correct response)*
- ☑ Use of Portable Electronic Devices *(correct response)*
- ☑ How to handle classified documents, such as procedures and equipment for accessing and photocopying, as well as storage *(correct response)*
- ☑ Policy and procedures for transmitting and/or transporting classified material *(correct response)*
- ☑ Reporting requirements for security violations *(correct response)*
- ☑ How to verify another person's PCL and need-to-know at the host facility prior to a classified discussion *(correct response)*

Feedback: *All of the topics listed may be presented in the security briefing for visitors.*

Review Activity 4

Which of the following are access controls appropriate for a classified visit?

- ☑ Control visitor activities so they have access only to classified information consistent with the authorized purpose of the visit *(correct response)*
- ☐ Prevent the visitor from accessing classified information in the secure storage cabinet
- ☑ Ensure unauthorized persons cannot overhear classified discussions for which they are not cleared and do not have a need-to-know *(correct response)*

Feedback: *The host organization must control visitor activities so they have access only to classified information consistent with the authorized purpose of the visit and ensure unauthorized persons cannot overhear classified discussions for which they are not cleared and do not have a need-to-know.*

Review Activity 5

When the purpose of the visit has been accomplished, or at the close of each day, what's the final security control?

- ○ Ensure the classified documents have the proper cover page and are placed in a desk file folder for work/use the next day.
- ⊙ Recover all classified and store/secure in security container or approved area. (correct response)
- ○ Verify documents have not been altered before they leave the facility.

Feedback: *The final security control is the recovery of all classified information when the purpose of the visit has been accomplished or, for visits of more than one day, at the close of each business day, ensure that classified material has been properly stored and that the security container has been secured.*

Review Activity 6

Which of the following are best practices for maintaining security control over classified information?

- ☑ Require visitors to sign a visitor record or log. *(correct response)*
- ☑ Provide visitors with a badge and an escort when in areas where classified information may be subject to unauthorized disclosure. *(correct response)*
- ☑ Use a card access system. *(correct response)*
- ☑ Have clear policies on sanitizing the work area. *(correct response)*

Feedback: *Though not required, all of these are best practices for maintaining security control during classified visits.*

Lesson 5 Review Activities

Review Activity 1

Which of the following are host organization requirements and security controls for an incoming international visit?

1 of 4. Obtain an export authorization for discussion of classified information. *(correct response)*

Feedback: *Access control procedures should ensure that the disclosure of, and access to, export-controlled articles and related information is limited to those that are approved by an export authorization.*

2 of 4. Prepare a Technology Control Plan (TCP) for long-term visitors. *(correct response)*

Feedback: *A TCP is required to control access by foreign nationals assigned to, or employed by, cleared contractor facilities.*

3 of 4. Implement access controls to limit disclosure to export authorization. *(correct response)*

Feedback: *Contractors hosting incoming foreign visitors must implement procedures to prevent access to controlled information beyond the approved scope of the visit.*

4 of 4. Maintain a visitor record. *(correct response)*

Feedback: *Contractors hosting foreign visitors must maintain a record of foreign visitors for five years when the visit involves classified information.*

Review Activity 2

Which of the following are the steps for an outgoing international visit?

- ☐ The U.S. contractor submits a Request for Visit (RFV) through the Foreign Visits System (FVS).
- ☑ The U.S. contractor faxes the RFV to DCSA Headquarters. *(correct response)*
- ☑ The RFV is forwarded by DCSA Headquarters to the U.S. Embassy in the foreign country to be visited. *(correct response)*
- ☐ The U.S. Embassy forwards the approved RFV to the visit site.
- ☑ The U.S. Embassy forwards the RFV to the foreign government office for approval. *(correct response)*
- ☑ The foreign government office sends the approved RFV to the visit site. *(correct response)*

Feedback: *The U.S. contractor faxes the RFV to DCSA Headquarters. The RFV is then forwarded by DCSA Headquarters to the U.S. Embassy in the foreign country to be visited. The U.S. Embassy will then forward the RFV to the foreign government office for approval—who in turn will send the approved RFV to the visit site.*

Review Activity 3

A foreign national is being assigned to work with your company and requires extended visit approval.

Select all the steps of the incoming international visit approval process.

- ☑ The foreign government office may submit a Request for Visit (RFV) through the Foreign Visits System (FVS). *(correct response)*
- ☑ The foreign government office may submit an RFV to the DCSA Headquarters.
- ☑ The foreign government office may submit an RFV to its embassy in Washington, D.C. *(correct response)*
- ☑ The foreign government office submits a written confirmation of security assurance. *(correct response)*
- ☑ Once the RFV is approved, DCSA Headquarters notifies the U.S. contractor.

Feedback: *RFVs are submitted by the foreign government office directly into the FVS or to their embassy in Washington, D.C., which forwards it for processing through DOD's International Visits Program (IVP). The foreign government must also submit a written confirmation of security assurance.*

Review Activity 4

Which of the following are requirements and security controls for NATO visits involving classified information at a U.S. facility?

- ☐ Obtain written consent of NATO member's government
- ☑ Maintain visitor records for three (3) years *(correct response)*
- ☐ Provide a declination notice to the foreign government
- ☑ Annual security briefings and exit debrief with signed certificate *(correct response)*
- ☑ Export authorization *(correct response)*
- ☑ Obtain a Facility Security Clearance Certificate (FSCC) from the CSA *(correct response)*

Feedback: *Visitor records must be maintained on all visitors to NATO sites for three (3) years. Visitors must sign a certificate for annual refresher briefings on NATO procedures and must have an exit debrief. Contractors must submit a request for export authorization and obtain an FSCC from the CSA equivalent to the U.S. FCL.*

Lesson 6 Review Activities

Review Activity 1

For each listed procedure or security control, identify which entity is responsible.

1 of 5. Verify Personnel Security Clearance (PCL) and need-to-know

- ☑ Government Contracting Activity (GCA) *(correct response)*
- ☐ Hosting Organization
- ☐ Participant / Presenter

Feedback: *The GCA must verify PCLs and need-to-know through the DOD System Personnel Security System of Record.*

2 of 5. Verify Facility Clearance (FCL)

- ☑ Government Contracting Activity (GCA) *(correct response)*
- ☐ Hosting Organization
- ☐ Participant / Presenter

Feedback: *The GCA verifies the FCL System of Record.*

3 of 5. Provide security classification guidance on information presented

- ☐ Government Contracting Activity (GCA) *(correct response)*
- ☐ Hosting Organization
- ☑ Participant / Presenter *(correct response)*

Feedback: *The presenters of classified information must provide attendees with security classification guidance on the information presented.*

4 of 5. Collect, safeguard, and transmit classified notes or recordings

- ☐ Government Contracting Activity (GCA)
- ☑ Hosting Organization *(correct response)*
- ☐ Participant / Presenter

Feedback: *The hosting organization must ensure notes and recordings are classified, safeguarded and transmitted according to the NISPOM.*

5 of 5. Obtain authorization for disclosure of classified information from the agency with jurisdiction over it

- ☐ Government Contracting Activity (GCA)
- ☐ Hosting Organization
- ☑ Participant / Presenter *(correct response)*

Feedback: *Participants and presenters must obtain prior written authorization for any proposed disclosure from the agency with jurisdiction over that classified information.*

Review Activity 2

Which of the following are responsibilities of the Government Contracting Activity (GCA) in sponsoring contractor proposed classified meetings?

- ☑ Ensure the meeting serves a government purpose *(correct response)*
- ☐ Provide a declination notice to the foreign government
- ☑ Process the contractor's request for authorization *(correct response)*
- ☑ Ensure adequate security measures are provided in advance, including announcements, requisite participant clearance and need-to-know, and compliance with presentation material requirements, and physical security measures are in place
- ☑ Evaluate and approve the proposed location *(correct response)*
- ☐ Ensure the announcement specifies the security clearances, justification to attend, and topics to be discussed in classified sessions

Feedback: *The GCA is responsible for the following: Ensure the meeting serves a government purpose; process the contractor's request for authorization; ensure adequate security measures have been provided in advance, including announcements, requisite participant clearance and need-to-know, and compliance with presentation material requirements, and physical security measures are in place; and evaluate and approve the proposed location.*

Review Activity 3

Which of the following are steps involved for a contractor to host GCA-sponsored meetings?

- ☑ Submit a request for authorization to the government agency that has agreed to assume security jurisdiction *(correct response)*
- ☐ Obtain a Facility Security Clearance Certificate (FSCC) from the CSA
- ☑ Issue an announcement or invitation to non-foreign visitors once the request to host a classified meeting is granted *(correct response)*

Feedback: *Cleared contractors that want to host GCA-sponsored meetings must submit a request for authorization to the government agency that has agreed to assume security jurisdiction and, once the request to host a classified meeting is granted, issue an announcement or invitation to non-foreign visitors.*

Review Activity 4

Which of the following are disclosure authority requirements for contractors desiring to disclose classified information at a meeting?

- ☑ Obtain prior written authorization for each proposed disclosure from the government agency having jurisdiction over the information *(correct response)*
- ☐ Obtain a Facility Security Clearance Certificate (FSCC) from the CSA
- ☑ Furnish a copy of the disclosure authorization to the government agency sponsoring the meeting *(correct response)*

Feedback: *Contractors desiring to disclose classified information at a meeting must obtain prior written authorization for each proposed disclosure from the government agency having jurisdiction over the information and furnish a copy of the disclosure authorization to the government agency sponsoring the meeting.*

Review Activity 5

Which of the following are security control responsibilities for hosting a classified meeting?

- ☑ Obtain prior written authorization for each proposed disclosure from the agency with jurisdiction over the information *(correct response)*
- ☑ Implement physical security measures approved by the GCA for control of, access to, and dissemination of, the classified information to be presented *(correct response)*
- ☑ Provide for secure storage capability, if necessary *(correct response)*
- ☑ Ensure security classification guidance on information presented *(correct response)*
- ☑ Ensure presentation delivery is oral/visual *(correct response)*
- ☐ Distribute classified presentations at the meeting
- ☑ Ensure notes and recordings are appropriately marked, safeguarded, and transmitted according to the NISPOM *(correct response)*

Feedback: *Security control responsibilities for hosting a classified meeting include: (1) Obtain prior written authorization for each proposed disclosure from the agency with jurisdiction over the information; (2) Implement physical security measures approved by the GCA for control of, access to, and dissemination of, the classified information to be presented; (3) Provide for secure storage capability, if necessary; (4) Ensure security classification guidance on information presented; (5) Ensure presentation delivery is oral/visual; and (6) Ensure notes and recordings are appropriately marked, safeguarded, and transmitted according to the NISPOM.*