

Visits and Meetings in the NISP

Student Guide

March 2026

Table of Contents

Lesson 1: Course Introduction 1

Lesson 2: Classified Meetings 3

Lesson 3: Classified Visit Basics 9

Lesson 4: Procedures for Classified Visits 14

Lesson 5: Security Controls During Classified Visits 20

Lesson 6: Course Conclusion 22

Appendix A: Answer Key—Review Activities A-1

Lesson 1: Course Introduction

Course Introduction

Lesson Overview

Welcome to the Visits and Meetings in the NISP Course. This course will help you understand the National Industrial Security Program (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.

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 32 Code of Federal Regulations (CFR) Part 117, National Industrial Security Program Operating Manual (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 meetings and then we will turn your attention to classified visits in the remaining lessons. Visits and meetings that involve disclosure of classified information require security professionals to understand the procedures in the 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.

Course Objectives

Here are the course objectives:

- Identify the requirements for classified visits in the National Industrial Security Program (NISP)
- Identify and describe the roles and responsibilities associated with sponsoring and hosting classified meetings

- Explain the difference between responsibilities and procedures for sending an employee on a classified visit versus hosting a classified visit
- Describe the requirements and best practices for maintaining security controls in the NISP

Course Lessons

This course is organized into the lessons listed here:

- Course Introduction
- Classified Meetings
- Classified Visit Basics
- Procedures for Classified Visits
- Security Controls During Classified Visits
- Course Conclusion

Lesson 2: Classified Meetings

Introduction

Lesson Overview

Classified meetings are sponsored by the Government Contracting Activity (GCA). Meetings often represent different Government organizations and cleared contractor facilities at a conference, seminar, symposium, exhibit, convention, training course, or other event 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. To be a classified meeting under the National Industrial Security Program Operating Manual (NISPOM), the gathering must be sponsored by a Government agency to serve a Government purpose.

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

Meetings Overview

GCA Role

Classified meetings are sponsored by a Government agency to serve a Government purpose. Cleared contractors can host these meetings if a Government agency has authorized it and assumes security jurisdiction. However, disclosure of classified information to larger, 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 (PCLs), in the DOD Personnel Security System of Record, as well as their justification for attendance.

Additionally, all persons attending classified sessions must have a need-to-know for the information to be disclosed. A need-to-know may be determined by the authorizing agency or its designee based on the justification provided.

Justification Requirements

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

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

Holding a Classified Meeting

Request for Authorization

Cleared contractors may host GCA-sponsored meetings. 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 should also include specifics on the subject, scope, security classification levels, security arrangements, dates and location, and attendees. The attendees listed should include any non-Government organizations involved, including a full description of the type of support it will provide. Any proposed foreign representatives, including their nationality, name, and organizational affiliation should also be listed.

Announcements/Invitations

If a cleared contractor's request to host a classified meeting is granted, an announcement or invitation is issued. It will 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 is authorized to provide. These statements include that only the Government agency has authorized the conduct of classified sessions, will provide necessary security assistance, and will forward the participants' security clearances and justifications to attend the meeting to the authorizing agency or its designee. Invitations to *foreign* visitors are issued by the authorizing Government agency, *not* the hosting contractor.

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 (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.

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 sent to the Government agency sponsoring the meeting.

Meeting attendees must present official identification, such as a passport, or U.S. Government ID card, to enter the session. Presentations must contain appropriate security classification guidance so that attendees know what information is classified and the level of classification. Presentations must be delivered orally 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:
 - Obtain prior written authorization for each proposed disclosure of classified information from the Government agency having jurisdiction over the information involved.
 - Send a copy of the disclosure authorization to the Government agency sponsoring the meeting.
- 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.

Host Organization Security Control Responsibilities

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 for 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.

If necessary, the host organization must also provide secure storage capability for classified documents. Consult the Technology Control Plan (TCP) if applicable. Host organizations must ensure any classified notes or electronic recordings of classified presentations be 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

Which entity is responsible for verifying Personnel Security Clearance (PCL) and need-to-know?

- Government Contracting Activity (GCA)
- Hosting Organization
- Participant / Presenter

Review Activity 2

Which entity is responsible for collecting, safeguarding, and transmitting classified notes or recordings according to the NISPOM?

- Government Contracting Activity (GCA)
- Hosting Organization
- Participant / Presenter

Review Activity 3

Before disclosing classified information at a meeting, written authorization must be obtained from:

- The Government agency having jurisdiction over the information involved
- Hosting Organization
- Participant / Presenter

Review Activity 4

Which of the following are responsibilities of the Government Contracting Activity (GCA) sponsoring a classified meeting? *Select all that apply.*

- Ensure the meeting serves a Government purpose
- Provide a declination notice to a foreign government
- Authorize the cleared contractor to host the meeting
- Assume security jurisdiction
- Approve security arrangements, announcements, attendees, and the location of the meeting

Review Activity 5

Which of the following are security control responsibilities for hosting a classified meeting?
Select 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
- Distribute classified presentations at the meeting
- Ensure notes and recordings are appropriately marked, safeguarded, and transmitted according to the NISPOM

Lesson 3: Classified Visit Basics

Introduction

Industry and Government workers supporting a classified contract may have to visit one another's facilities to discuss a project. An important aspect of your role as a Facility Security Officer (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 (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. To learn about classified international and North Atlantic Treaty Organization (NATO) visits, please refer to the Course Resources page.

Lesson Objective

- Identify the requirements for classified visits in the NISP

Basic Concepts

Characteristics of Classified Visits

The purpose of a classified visit is to share classified information between two or more people. In most cases, a visitor is an individual who is authorized to access classified information for a Government purpose.

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.

Visits have requirements for the disclosure of classified information!

Uncleared Visitors

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.

An uncleared visitor is an individual who:

- Needs access to a classified area
- Cannot be isolated from classified information

Ideally, an area would be sanitized of all classified material and a cleared employee would escort the uncleared visitor to prevent them from having access to classified information. In some cases though, the nature of the visit could mean that it is not possible to take these measures. For example, a maintenance person may have to enter a classified area to repair a piece of equipment that cannot be removed.

If a visitor cannot be excluded from access, all relevant requirements in the NISP must be met.

The escort must be properly cleared and must have enough knowledge of what is classified to prevent the uncleared person from accessing 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.

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 6-month or 1-year timeframe. Long-term visits occur when the contractor employee is 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 the 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.

NISP Requirements for Classified Visits

Authorization Requirements

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 (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 of, or possession of the information to perform tasks or services essential to the fulfillment of a classified contract or program.

Need-to-Know

- Person has a need-to-know when they require access to, knowledge of, or possession of classified information to perform tasks or services essential to the fulfillment of a classified contract or program
- Determination of an individual's need-to-know rests with the entity disclosing the information
- Determination is generally based on a contractual relationship and documented in the DD Form 254

NISP Classified Visit 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. 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 disclosure of, classified information.

For a visit request to be approved, the host organization must ensure that the visitor's identity is confirmed and that they have the proper PCL and need-to-know prior to the disclosure of any classified information. The host organization is responsible for ensuring that the 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 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

Regardless of the visit duration, all visitors, whether Government employees or contractors, must follow the host organization's security procedures. *Select the best response.*

- True
- False

Review Activity 2

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. *Select the best response.*

- True
- False

Review Activity 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. *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 authorized 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 for the classified information in the performance of official duties.

Review Activity 5

Which of the following are the 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 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 Personnel Security Clearance (PCL) and need-to-know.

Lesson 4: Procedures for Classified Visits

Introduction

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

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

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 Personnel Security Clearance (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 (VAL) provided 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 is used to decide whether a person may be granted access to classified information. The system is utilized by Facility Security Officers (FSOs) and designated security personnel, Defense Counterintelligence and Security Agency Industrial Security Representatives (DCSA ISRs) 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.

VAL Method

The alternate method for a visit authorization is the VAL, which is provided by the visitor's organization. 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, determining if 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.

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, Commercial and Government Entity (CAGE) Code, if applicable, and certification of the level of the favorable entity eligibility determination, also referred to as a FCL.

Second, 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 fourth element is the name of the person, or persons, to be visited, and the fifth element must address the *necessity* for the visit, stating its purpose and justification, including the specific contract number, project, or program number.

Finally, the VAL must indicate the date or period during which it is valid.

VAL Transmission

A VAL may be sent via U.S. Postal mail or overnight mail, fax, or via email. When using electronic means, access to the VAL must be controlled through physical or software protection and have digital signature authentication. 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 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.

Organization Roles

Visitor Organization

When sending an individual on a classified visit at another facility, the visitor organization and the host organization have several responsibilities. In accordance with the NISPOM's requirement to keep the number of visits to a minimum, the visitor 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 encounter classified information? 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 in the applicable system of record and on the VAL.

Note: Report 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 host point-of-contact and the project manager or other subject-matter expert to determine if it is in the interest of the Government to approve this classified visit. This individual 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 no contractual relationship, the host organization must obtain authorization to disclose the classified information from the 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

Whose responsibility is it to verify visitors' appropriate Personnel Security Clearance (PCL)? *Select all that apply.*

- Visitor Organization
- Host Organization

Review Activity 2

Whose responsibility is it to determine a need-to-know? *Select all that apply.*

- Visitor Organization
- Host Organization

Review Activity 3

Whose responsibility is it to determine the need for a classified visit? *Select all that apply.*

- Visitor Organization
- Host Organization

Review Activity 4

Whose responsibility is it to send the Visit Authorization Letter (VAL)? *Select all that apply.*

- Visitor Organization
- Host Organization

Review Activity 5

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

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

Lesson 5: Security Controls During Classified Visits

Introduction

During classified visits, visitors must follow the host organization's security controls. The 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.

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 (VAL) or in the DOD Personnel Security System of Record. Then, each visitor's identity must be verified. Official identification must contain both the person's name and photo, such as a driver's license, passport, or USG 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.

Security Briefings

It is a good security practice for the host organization to review the security procedures a visitor will be expected to follow with a security briefing, and keep a record of that briefing. 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 (PEDs) such as cell phones, tablets, laptops, video and audio recording and playback devices, and smart watches.

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 transporting classified material. This is especially relevant to long-term visitors who are typically working on-site at the host facility. Finally, the security briefing may cover the reporting requirements for security violations, such as loss or compromise of classified material.

When a Visit Authorization Request (VAR) is sent using the DOD Personnel Security System of Record 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.

Visitor Access Controls

The host must control the activities of visitors so they only have access 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.

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 for 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 visitor badge and an escort. When needed, the escort must be an appropriately cleared employee who has been briefed on the access limitations and 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.*

- Call the visitor's company to verify the 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 visitor access
- Ask the visitor if they have a need-to-know for the classified information

Review Activity 2

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
- Policy and procedures for handling, transmitting, and/or transporting classified material
- Reporting requirements for security violations

Review Activity 3

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

- Control visitor activities so they only have access 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 4

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 information and store/secure in an approved security container or area.
- Verify documents have not been altered before they leave the facility.

Review Activity 5

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

- Request that visitors sign a visitor record or log.
- Provide visitors with a visitor badge and an escort.
- Use a card access system.
- Have clear policies on sanitizing the work area.

Lesson 6: Course Conclusion

Conclusion

Summary

Visits and meetings in the National Industrial Security Program (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.

Course Objectives

You should now be able to:

- Identify the requirements for classified visits in the National Industrial Security Program (NISP)
- Identify and describe the roles and responsibilities associated with sponsoring and hosting classified meetings
- Explain the difference between responsibilities and procedures for sending an employee on a classified visit versus hosting a classified visit
- Describe the requirements and best practices for maintaining security controls in the NISP

Congratulations. You have completed reading the Visits and Meetings in the NISP Student Guide. To receive course credit, you **MUST** take the Visits and Meetings in the NISP examination. Follow the instructions in the STEPP system to access the online exam.

Appendix A: Answer Key—Review Activities

Lesson 2 Review Activities

Review Activity 1

Which entity is responsible for verifying Personnel Security Clearance (PCL) and need-to-know?

- Government Contracting Activity (GCA)
- Hosting Organization
- Participant / Presenter

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

Review Activity 2

Which entity is responsible for collecting, safeguarding, and transmitting classified notes or recordings according to the NISPOM?

- Government Contracting Activity (GCA)
- Hosting Organization
- Participant / Presenter

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

Review Activity 3

Before disclosing classified information at a meeting, written authorization must be obtained from:

- The Government agency having jurisdiction over the information involved
- Hosting Organization
- Participant / Presenter

Feedback: Prior to disclosure of classified information, written authorization must be obtained from the Government agency with jurisdiction over the classified information.

Review Activity 4

Which of the following are responsibilities of the Government Contracting Activity (GCA) sponsoring a classified meeting? *Select all that apply.*

- Ensure the meeting serves a Government purpose
- Provide a declination notice to a foreign government
- Authorize the cleared contractor to host the meeting
- Assume security jurisdiction
- Approve security arrangements, announcements, attendees, and the location of the meeting

Feedback: *The GCA is responsible for the following: Ensure the meeting serves a Government purpose; authorize the cleared contractor to host the meeting, assume security jurisdiction, and approve security arrangements, announcements, attendees, and the location of the meeting.*

Review Activity 5

Which of the following are security control responsibilities for hosting a classified meeting? *Select 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
- Distribute classified presentations at the meeting
- Ensure notes and recordings are appropriately marked, safeguarded, and transmitted according to the NISPOM

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 and (4) Ensure notes and recordings are appropriately marked, safeguarded, and transmitted according to the NISPOM.*

Lesson 3 Review Activities

Review Activity 1

Regardless of the visit duration, all visitors, whether Government employees or contractors, must follow the host organization's security procedures. *Select the best response.*

- True
- False

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

Review Activity 2

When a contractor employee visits a Government facility, he or she must follow the security requirements of that facility and the visitor organization is relieved from continued security oversight of that employee. *Select the best response.*

- True
- False

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

Review Activity 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. *Select the best response.*

- True
- 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 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 authorized 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 for the classified information in the performance of official duties.

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

Review Activity 5

Which of the following are the 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 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 Personnel Security Clearance (PCL) and need-to-know.

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 4 Review Activities

Review Activity 1

Whose responsibility is it to verify visitors' appropriate Personnel Security Clearance (PCL)? *Select all that apply.*

- Visitor Organization
- Host Organization

Feedback: *The host organization must verify visitors' appropriate PCL.*

Review Activity 2

Whose responsibility is it to determine a need-to-know? *Select all that apply.*

- Visitor Organization
- Host Organization

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

Review Activity 3

Whose responsibility is it to determine the need for a classified visit? *Select all that apply.*

- Visitor Organization
- Host Organization

Feedback: *Both the visitor 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.*

Review Activity 4

Whose responsibility is it to send the Visit Authorization Letter (VAL)? *Select all that apply.*

- Visitor Organization
- Host Organization

Feedback: *The visitor organization sends the Visit Authorization Letter (VAL).*

Review Activity 5

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

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

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

Lesson 5 Review Activities

Review Activity 1

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

- Call the visitor's company to verify the 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 visitor access.
- Ask the visitor if they have a need-to-know for the classified information

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

Review Activity 2

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
- Policy and procedures for handling, transmitting, and/or transporting classified material
- Reporting requirements for security violations

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

Review Activity 3

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

- Control visitor activities so they only have access 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

Feedback: *The host organization must control visitor activities so they only have access 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 4

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 information and store/secure in an approved security container or area.
- 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, ensuring that classified material has been properly stored, and that the security container/area has been secured.*

Review Activity 5

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

- Request that visitors sign a visitor record or log.
- Provide visitors with a visitor badge and an escort.
- Use a card access system.
- Have clear policies on sanitizing the work area.

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