

Student Guide

Course: Visits and Meetings in the NISP

Lesson: Foreign and NATO Visits

Lesson 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 foreign and NATO visits as outlined in the National Industrial Security Program Operating Manual (NISPOM), Chapter 10: International Security Requirements, Section 5: International Visits and Control of Foreign Nationals and Department of Defense Directive 5230.20, Visits and Assignments of Foreign Representatives. The lesson will explore the approval process for incoming and outgoing visitors and required security controls.

The lesson objectives are:

- Identify the requirements and security controls for incoming and outgoing foreign visits
- Identify the process for foreign visit approval including the role of the contractor, embassy, and foreign visits system (FVS)
- Identify the requirements and security controls for NATO visits

NISP Foreign Visit Policy

1. International Visits Overview

As you learn about the NISP foreign visit policies, there are three key visit relationships this course 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 (NATO) related visits. Visits by foreign nationals or representatives of a foreign government to U.S. contractor facilities are called incoming foreign visits. Visits abroad by U.S. contractors are referred to as outgoing foreign 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 has 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 (CUI). This course will discuss each category and outline the applicable requirements and procedures.

2. Visit Duration

International visits can take place over different time periods. The NISPOM (Chapter 10: International Security Requirements, Section 5: International Visits and Control of Foreign Nationals) 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 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. 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 (GCA) of the industrial facility to be visited to ensure the emergency visit request has all the necessary details.

Emergency Letter Requirements:

- Use letter or email format:
 - It must be from one of the following:
 - Point of contact (POC) in Block 3 of the visit request form
 - Military POC
 - NATO site
 - Embassy of the country to be visited
- Provide visitor name, position, address, and phone
- Identify contract, agreement, or program
- Provide justification for the visit:
 - State the significant nature of the visit
 - Express that it cannot be rescheduled
- Identify beginning and ending dates of visit

Incoming Foreign Visits

1. 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 (Chapter 10, International Security Requirements), 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 (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 you are seeking to comply with.

2. Visit Procedures and Requirements

Incoming foreign visits require the sponsoring foreign government to submit a request for a classified visit (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.

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

Per the NISPOM (Para. 10-507(c). Non-Sponsorship), 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.

Contractors must establish procedures to monitor incoming foreign 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.

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. (NISPOM, 10-501(b))
- 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.” (NISPOM, 10-507)

For long-term foreign visitors or employees, contractors should document procedures in a technology control plan (TCP). In the event the Government does *not* approve the incoming foreign visit, different requirements apply.

3. Approval Process

The DoD International Visits Program (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 (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 with any 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.

Security Controls During Foreign Visits

1. Security Controls

Security controls for international visits are required to protect the nation's sensitive information as outlined in the NISPOM (Para. 10-507(e), Visitor Records and Para. 10-509, TCP).

Contractors must maintain a record of foreign visitors 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.

Employees traveling overseas must receive threat awareness, antiterrorism/force protection, and countermeasures security briefings.

Security briefings:

- Some information for the threat awareness and antiterrorism/force protection security briefing should be available from the host organization prior to the visit.
- Anti-terrorism (AT) Level One training is available online at <https://atlevel1.dtic.mil/at/>
- The FSO may also have to do some research on the threat in the area to be visited as well as resources available to the traveler when in that area. Resources are available from many U.S. Government agencies.

Contractors must also establish procedures to monitor their employees' international visits. These access control procedures should ensure that disclosure of, and access to, export-controlled articles and related information is limited to what is approved in the export authorization.

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 (TCP).

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
- Examples of these incidents are on the DSS website

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 Industrial Security (IS) Rep at the Defense Security Service. Reports of actual, probable, or possible espionage, sabotage, terrorism, or subversive activities should be reported to the FBI with a copy to the DSS IS Rep.

Purpose of the TCP:

- 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

2. 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 technology control plan.

Outgoing Foreign Visits

1. Visit Requirements

The NISPOM (Paragraph 10-506, Visits Abroad by U.S. Contractors, Appendix B: International Visits Standard RFV) provides guidance on visits abroad by U.S. contractors, or outgoing visits. International visits must meet the NISPOM requirements whether the information is classified or is unclassified information related to classified contracts or otherwise 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 (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.

2. Approval Process

Requests for outgoing visits must be faxed to the Defense Security Service (DSS) Headquarters, International Division. The International Division 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, DSS Headquarters, International Division 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.

NATO Visits

1. Overview of NATO-Related Visits

Per the NISPOM (Chapter 10: International Visits and Control of Foreign Nationals, Section 7, NATO Information Security Requirements), in order for a contractor to negotiate or perform on a NATO classified contract, it must have a NATO Facility Security Clearance Certificate (FSCC). A U.S. facility qualifies for a NATO FSCC, if it has an equivalent U.S. facility clearance and has briefed personnel on NATO procedures. The DoD cognizant Security office for DoD employees or the DSS Headquarters, International Division for contractor employees 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 at the equivalent level and must have received a NATO Briefing and signed a NATO Briefing Certificate.

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

(NISPOM, 10-701. Classification Levels)

2. Approval Process

The NATO visit approval process is slightly simpler than for foreign outgoing visits. The request to visit a NATO site is still processed through DSS Headquarters, International Division.

The difference is that DSS Headquarters, International Division sends the approval directly to the NATO site.

3. Security Controls

Per the NISPOM (Chapter 10, International Security Requirements, Section 7, NATO Information Security Requirements), contractors are required to maintain a separate record of NATO visits, including those by U.S. personnel assigned to NATO. Those records must be kept for five years. Employees must be given an initial NATO security briefing covering topics on access, preparing and marking NATO documents, storage, distribution, handcarrying, and reproduction. Employees must also receive annual refresher briefings and a debriefing. The employee must sign a certificate stating that the briefings were received and acknowledge personal responsibility for safeguarding NATO information. This certificate is maintained for two or three years, depending on the classification level of the information accessed. Release of U.S. classified or export-controlled information to NATO requires an export authorization or other written disclosure authorization.

Review Activity

Try answering the following questions. When you are finished, see the Answer Key at the end of this Student Guide to check your answers.

Question 1

Identify whether each listed requirement applies to incoming or outgoing foreign visits, or both. Check your answers in the Answer Key at the end of this Student Guide.

Requirements	Incoming Foreign Visits	Outgoing Foreign Visits
Obtain an export authorization for discussion of classified information	<input type="checkbox"/>	<input type="checkbox"/>
Prepare a Technology Control Plan (TCP) for long-term visitors	<input type="checkbox"/>	<input type="checkbox"/>
Implement procedures to prevent visitors from access to controlled information beyond the approved scope of the visit	<input type="checkbox"/>	<input type="checkbox"/>
Maintain a visitor record	<input type="checkbox"/>	<input type="checkbox"/>
Provide threat awareness training	<input type="checkbox"/>	<input type="checkbox"/>
Provide antiterrorism/force protection security briefing	<input type="checkbox"/>	<input type="checkbox"/>

Question 2

One of your company's employees needs to meet with a subcontractor in England to iron out some technical issues on a state-of-the-art unmanned aerial vehicle project for a program administered by your Government Contracting Activity. Select the steps of the outgoing international visit approval process. Check your answers in the Answer Key at the end of this Student Guide.

- The U.S. contractor submits a Request for Visit (RFV) through the Foreign Visits System (FVS).
- The U.S. contractor faxes the RFV to DSS Headquarters, International Division.
- The U.S. contractor ensures the host coordinates with the government authorities who will approve the visit.
- DSS Headquarters, International Division submits a written confirmation of security assurance.
- The RFV is forwarded by DSS Headquarters, International Division to the U.S. Embassy in London.
- The U.S. Embassy forwards the approved RFV to the visit site in England.

- 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.

Question 3

A foreign national is being assigned to work with your company and requires extended visit approval. Select the steps of the incoming international visit approval process. Check your answers in the Answer Key at the end of this Student Guide.

- 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 DSS Headquarters, International Division.
- The foreign government office may submit an RFV to its embassy in Washington, DC.
- The foreign government office submits a written confirmation of security assurance to DoD's International Visits Program (IVP).
- The foreign government office submits a confirmation of security assurance to DSS Headquarters, International Division.
- Once the RFV is approved, DSS Headquarters, International Division notifies the U.S. contractor.
- Once the RFV is approved, DoD's International Visits Program notifies the U.S. contractor.

Question 4

Which of the following are requirements and security controls for NATO visits involving classified information at a U.S. facility? Check your answers in the Answer Key at the end of this Student Guide.

- Obtain written consent of NATO member's government
- Maintain visitor records for five 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 Conclusion

In this lesson, you learned the requirements and security controls for incoming and outgoing foreign visits, including the importance of the technology control plan, how to

handle extended visits, visits by non-U.S. citizens, and visits deemed non-sponsored. You also examined the process for foreign visit approval including the role of the contractor, embassy, and foreign visits system (FVS). Finally, you explored the requirements and security controls for NATO visits.

Answer Key

Question 1

Requirements	Incoming Foreign Visits	Outgoing Foreign Visits
Obtain an export authorization for discussion of classified information	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Prepare a Technology Control Plan (TCP) for long-term visitors	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Implement procedures to prevent visitors from access to controlled information beyond the approved scope of the visit	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Maintain a visitor record	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Provide threat awareness training	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Provide antiterrorism/force protection security briefing	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Question 2

- The U.S. contractor submits a Request for Visit (RFV) through the Foreign Visits System (FVS).
- The U.S. contractor faxes the RFV to DSS Headquarters, International Division.
- The U.S. contractor ensures the host coordinates with the government authorities who will approve the visit.
- DSS Headquarters, International Division submits a written confirmation of security assurance.
- The RFV is forwarded by DSS Headquarters, International Division to the U.S. Embassy in London.
- The U.S. Embassy forwards the approved RFV to the visit site in England.
- 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.

Question 3

- 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 DSS Headquarters, International Division.
- The foreign government office may submit an RFV to its embassy in Washington, DC.
- The foreign government office submits a written confirmation of security assurance to DoD's International Visits Program (IVP).
- The foreign government office submits a confirmation of security assurance to DSS Headquarters, International Division.
- Once the RFV is approved, DSS Headquarters, International Division notifies the U.S. contractor.
- Once the RFV is approved, DoD's International Visits Program notifies the U.S. contractor.

Question 4

- Obtain written consent of NATO member's government
- Maintain visitor records for five 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