

LESSON 8

Security Education: Briefings

You can't do it all. You can't do it alone. Security won't happen at your facility unless the people there make it happen. For your security program to succeed, your people must know what is expected of them; what their security responsibilities are and what security procedures they must follow. The NISPOM requires you to accomplish these educational goals by conducting various briefings. These are usually small groups or one-on-one sessions in which you inform cleared persons of their security obligations and instruct them in security procedures.

OBJECTIVES

When you have completed this lesson, you should be able to do the following:

- Differentiate between an initial company briefing and the required initial security briefing.
- Identify contents of the initial security briefing and the refresher briefing.
- Identify the basic responsibilities for cleared employees in safeguarding classified information.
- Explain procedures for the use of SF 312, (Classified Information Nondisclosure Agreement).

INITIAL COMPANY BRIEFING

Many medium to large companies choose to give **all new** employees, **cleared and uncleared**, an initial company briefing. In addition to specific company procedures and policies, this briefing may cover general security topics such as the wearing of identification badges, entrance and exit procedures and/or the authority of the security forces, and fire regulations. This briefing may also inform employees that the company is involved with classified information and explain to them what to do if they find classified information by accident. This briefing is *not* required by the NISPOM. However, many companies consider it essential to the orientation of new employees. For example, everyone who works for, or is temporarily assigned to a facility that possesses classified information should be told what to do if they find classified material unattended, **(bring it to the FSO)**.

INITIAL SECURITY BRIEFING

The initial security briefing *is* required (**3-106, NISPOM**). This briefing is given to cleared employees **prior** to them having access to classified information.

Before we look at what the initial security briefing entails, note that under paragraph **3-100 (NISPOM)** you need to advise employees of the matters we discussed in Lesson 4, including the 13 eligibility criteria listed on page 4-8. Prior to being granted access to classified information, an employee shall receive an initial security briefing that must include the following information:

1. **Threat Awareness Briefing.** This briefing should inform employees of techniques employed by foreign intelligence services to obtain classified information. Most of these techniques are well-known and their use is predictable. You should familiarize yourself with these techniques by reviewing the material available under the Counterintelligence section of the DSS website – www.dss.mil. The articles and publications posted provide you with informative information that you can use to instruct and motivate your cleared employees. Be sure to contact your IS Rep to request assistance in obtaining threat information that is relevant and available for your company. A DSS Counterintelligence Agent (CI) is also helpful and provide

additional threat information. You may also wish to contact your local FBI office and arrange to sponsor or participate in an Awareness of National Security Issues and Response (ANSIR) briefing. Finally, be sure to emphasize the employees' responsibility to report any suspicious contacts to you, the FSO, as defined in **1-302b, NISPOM**.

2. **Defensive Security Briefing.** During the initial security briefing the cleared employees should be made aware that they may be targeted by foreign intelligence services and must be cautious whenever they come in contact with foreigners, whether in the United States or abroad. If your company markets outside the US, stress that export controlled information may be at risk as well as classified information. Point out that unclassified information relating to a classified contract shall not be disclosed, or any information that falls under the International Traffic in Arms Regulation. Unclassified technical data may require government approval before release.

Providing security to America's secrets in an era of intense post-cold-war global competition is a great challenge. We suggest that you review your NISP-related contracts and work with your IS Representative to familiarize yourself with the particular restrictions that may apply to your employees' situations and to obtain disclosure guidance from appropriate agencies, such as the Office of Defense Trade Controls, the Department of State, the Office of Export Administration, and the Department of Commerce. Then brief your employees accordingly.

3. **Overview of the security classification system.** Tell the employees that information is classified under a series of executive orders, the most recent being Executive Order 12958, "Classified National Security Information," (as amended) and signed by President Bush effective 25 March 2003. Explain that E.O. 12958 sets up a uniform system for classifying, declassifying, and safeguarding national security information, that is, information relating to the national defense or foreign relations.

Point out that national security information becomes classified information by one of two processes: *original classification* and *derivative classification*.

Original classification is an initial determination (decision) that information is to be given the protection of an executive order. Only about 7,000 designated officials of the Executive Branch can make such a determination. These "original classification authorities" base their decisions on three criteria:

1. The information must be national security information.
2. The United States Government must own, have a proprietary interest in, or control the information.
3. It must be determined that unauthorized disclosure of the information would cause damage to the national security.

If the information in question meets the above criteria, then the original classifier determines at which level to classify the information, according to the extent of damage to the national security that unauthorized disclosure of the information would cause:

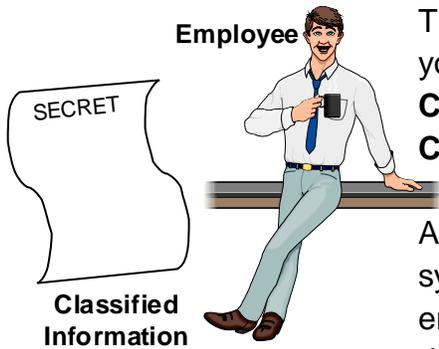
- **Damage** — CONFIDENTIAL
- **Serious Damage** — SECRET
- **Exceptionally Grave Damage** — TOP SECRET

Explain that derivative classification is performed in the course of their authorized functions by other government officials and by designated cleared employees at NISP facilities authorized to generate (produce) classified information.

Go on to explain that classified information must be handled only by appropriately cleared employees with a need-to-know, and that the NISPOM imposes strict requirements for the safeguarding and handling of classified information, including controls on its storage, receipt, distribution, use, generation, transmission, release, disclosure, and disposition.

Indoctrinate employees in the procedures for proper classification and marking of information and the safeguards necessary for accountability and control of classified information in the contractor's possession. Alert them to the strict prohibitions

against improper use and abuse of the classification system and familiarize them with the procedures for challenging classification decisions believed to be improper.



Employee

This is a tall order. If your facility possesses classified information, you will need to go over at least the requirements in **Chapter 4, Classification and Marking**, and **Chapter 5, Safeguarding Classified Information**, of the NISPOM.

Also, point out that E.O. 12958 prohibits use of the classification system to conceal violations of law, inefficiency, administrative error, and other such abuses. Challenges to classification decisions thought to be improper are made to the User Agency; the DSS Field Office may be asked to assist, if needed.

Level of Clearance



Need-to-Know



Authorized Person

You should also advise employees of the adverse affects to the national security that could result from unauthorized disclosure of classified information and of their personal, civic, and legal responsibility to protect classified information within their knowledge, possession, or control. You can paraphrase the descriptions of the three levels of classified information given in Lesson 1. You can refer to famous espionage cases where classified information was compromised (Ames, Walker, Boyce, Harper, Bell, Hanssen, and others). The espionage of CIA official Aldrich Ames and of John Walker and his family received media headlines for months.

If you're not familiar with the spying of Christopher Boyce, you can learn about it in Robert Lindsey's book, entitled, "*The Falcon and the Snowman*", which was made into a hollywood movie. You can order discussions of the Harper, Bell and other espionage cases from the Government Printing Office.

The descriptions of classified information come to life in the context of an espionage trial. Consider, for instance, the words of Judge Samuel Conti when sentencing James Harper to life imprisonment for selling US missile defense information to Polish agents. "Your actions have exposed all our people to risk and danger," he said, "a danger that could well extend into the 21st century. There can be no crime more serious than that of selling our country's defense secrets to a foreign government. Your crime

concerns each and every living and unborn citizen of this country," and it threatens "the very heart and existence of our freedom."

"It is ironic, indeed, that you pled guilty on April 15th, and that's the very day that all federal income taxes were due. It goes without saying that a great portion of the billions paid in taxes goes for national defense and yet you, for your own personal greed, would cause many of these billions to go for naught and to the advantage of a foreign power."

You may also wish to stress the importance of protecting classified information in terms of your company's retaining its FCL and its eligibility to work on defense contracts that provide jobs to its employees.

4. **Employee reporting obligations and requirements.** Inform employees of their *individual responsibility* for making reports to you, the FSO, as specified in the NISPOM. Briefly go over the types of situations that employees need to report to you so that you in turn can make the required reports as indicated in Lesson 6.
5. **Security procedures and duties applicable to the employee's job.** You might begin by advising the employees of the US Government requirements which must be met by a User Agency (UA) prior to disclosure of classified information to a contractor and the contractual obligations imposed when a contractor is given access to classified information. Explain that a UA must have a need for a product or service that entails the award of a classified contract (see Lesson 1). Explain that when a UA awards a classified contract to a contractor, the UA must incorporate a "Security Requirements Clause" and a "DoD Contract Security Classification Specification" (DD Form 254) in the contract. The DD Form 254 provides written notice of the security classification assigned to information generated by the contractor. Tell the employees that NISP contractors must comply with the classification guidance provided in the DD Form 254.

Inform all cleared employees of their responsibility for determining whether a prospective recipient of classified material is appropriately cleared and has a need-to-know for knowledge or

possession of the classified information and for advising the recipient of the classification of the information to be disclosed. Inform employees that unauthorized disclosure of classified information violates US Government regulations and contractual obligations and is punishable under federal law. Impress upon the cleared employees that when they gain knowledge of classified information, they become custodians of that information. Explain that knowledge or custody of classified information imposes two main obligations:

- 1) the ***disclosure decision***, and
- 2) the ***classification notification***.

The first of these obligations is spelled out in paragraph one of the Classified Information Nondisclosure Agreement (SF 312): "Intending to be legally bound, I hereby accept the obligations contained in this agreement in consideration of my being granted access to classified information, ect." Make it clear that divulging includes *oral disclosure* as well as transmitting classified information.

To nail down this obligation, emphasize this formula: ***Authorized Person = Clearance Level + Need-to-know***. Explain that this means that before employees disclose classified information to a prospective recipient the holder of the classified material must determine:

- 1) That the prospective recipient has a clearance at the level of the classified information in question (or at a higher level), and



When in doubt find out...

- 2) That the prospective recipient has a need-to-know, that is, the prospective recipient "has a requirement for access to, knowledge of, or possession of the classified information in order to perform tasks or services essential to the fulfillment of a classified contract or program approved by a User Agency."

Explain that the system at your facility or at a location where they will require access to classified material will allow them to determine quickly the *clearance level* of a prospective recipient.

Explain that the *need-to-know* determination can be more difficult. Emphasize the importance of forming the habit of asking cleared persons who request classified information: **"Why do you need to know this information?"** Tell the employees that they must be fully satisfied with the reason given or they must refuse to divulge the classified information. Stress the rule, "When in doubt, find out" by questioning the immediate supervisor of the person that will release the information. Explain that it is far better to delay disclosure to an authorized person than to disclose classified information to an unauthorized person.

Next, inform the employees that whenever they decide to disclose classified information, they must *advise the recipient of the classification level* of the information disclosed (e.g., "This information is classified SECRET").

It is recommended that your company provide employees with a copy of your company's Standard Practice Procedures (SPP). Review the portions that bear directly on the employees' duties and responsibilities. If no written SPP is available, provide employees with the specific security requirements for the job using any aids you may have prepared. For example, if you are briefing an employee who will primarily be concerned with visiting another cleared facility and will require access there, you would probably focus on the following:

- Your clearance (PCL) is at the [Top Secret/ Secret/Confidential] level.
- You will be at that facility for [time].

- You should *not* be given access to classified information at a higher level than your PCL level.
- You are required to comply with the security procedures at the host facility. You will be briefed on the host facility's security requirements and procedures.
- Don't discuss classified information outside of the work site or over a non-secure phone.
- You are authorized access to classified information at that location only.
- If you work at several places, don't discuss one place's classified information at another place, unless it has been authorized and is required by the terms of the contract.
- Don't accept classified documents that may be offered you to take back to your facility (if your facility is non-possessing).

If your firm possesses classified information and if practicable, you should accompany the employees to the work areas where they are assigned. Then you should explain and demonstrate the security procedures pertaining to that employee's particular job assignment. For instance, if an employee is an engineer, you might stress procedures regarding scientific meetings where representatives of foreign countries will attend and the procedures pertaining to "working papers". *Demonstrate* the correct way. Then have the employee do it and give the employee feedback. Remember that this briefing should be as specific and thorough as you can make it, with as much hands-on demonstration of security procedures as possible.

EXECUTION OF SF 312

Following the "initial security briefing" the employee(s) must read, understand and execute (sign) the Classified Information Nondisclosure Agreement, SF 312. The SF 312 is a legal document. By signing it, the employees formally certify that they have been made aware of their individual obligations regarding

classified information and of the penalties for violating these obligations.

When the employees sign the form, it is recommended that the employees' supervisor sign as the witness. **Ensure that employee and witness signatures bear the same date.** After obtaining all required signatures, send the SF 312 to DISCO.

If an employee refuses to execute the SF 312, deny the employee access to classified information and submit a report to DISCO, in accordance with Chapter 1-302g NISPOM.

Note: *NISPOM Paragraph 3-105 requires that an individual issued an initial personnel security clearance (PCL) execute an SF-312, Classified Information Nondisclosure Agreement **prior** to being granted access to classified information, and that the FSO submit the original SF-312 to DISCO for retention. Please note this requirement applies only to individuals granted **an initial PCL**. SF 312s for new employee(s) whose PCLs are restored resulting from conversions or reinstatements are not required to be sent to DISCO if one was previously executed and sent to DISCO.*

REFRESHER TRAINING



The **NISPOM, 3-107** requires that you give all cleared employees "some form of security education and training at least annually." Refresher training shall reinforce the information provided during the initial security briefing and shall keep cleared

employees informed of changes in security regulations. Stress their continuing responsibility to safeguard classified information. Review work assignment security procedures. Focus on any security problems noted during DSS reviews or self inspections that require their individual attention. Also, if there is a change in NISPOM requirements that affects your facility's operations, or if there is a change in operations inform the employees accordingly. Review the methods and operations used by foreign intelligence services to subvert US industrial personnel, and emphasize defensive measures that employees can take to counter these attempts. We suggest that to avoid boredom, vary your refresher training! Use the Internet to locate sources for security education materials. Begin your search with the DSS website (www.dss.mil) and join the membership of the Extranet for Security Professionals (www.xsp.org). The " Desk Top Resource Guide," available from your IS Rep, is a useful tool; it contains tips and techniques for creating an effective security education program. NOTE: Even though it's not required, It's a good idea to give your *uncleared employees* some type of security training. This training will be helpful to them in the future if they are promoted or transferred to an assignment that will require them to have access to classified information.

Helpful Hint: Vary your briefings to avoid boredom.

The **NISPOM, 3-107** requires that you "maintain records about the programs offered and employee participation in them. "Acceptable records include distribution lists, facility or department-wide newsletters, or other means that you, the FSO, find suitable.

SECURITY DEBRIEFING

The **NISPOM, 3-108** requires that you debrief all cleared employees who have had access to classified information to ensure that they are aware of their ***continuing responsibility*** to protect classified information.

You must debrief cleared employees when:

- The employee terminates employment, resigns, is discharged, or retires.*
- The employee's PCL is terminated.*
- The employee's PCL is suspended or revoked.
- Your company's FCL is terminated.

Note: If the employee has had access to information requiring special access authorization (e.g., COMSEC/NATO), you must give him or her an oral debriefing; see the charts at the end of this lesson.

For items asterisked above (), also send Form 562 to DISCO, as discussed in Lesson 5. (SF 312 debriefing is not required to be executed).*

SPECIAL BRIEFINGS

In addition to the basic briefings discussed so far, you may be required to provide other briefings as well. The following charts summarize these special briefings.

SPECIAL BRIEFINGS

Type	Reference	When to Give	Comments
<p>CNWDI Briefing</p>	<p>NISPOM, 9-202</p>	<p>Briefing of FSO: The facility's DSS representative will give the FSO a CNWDI briefing.</p> <p>Employee Briefings: The FSO or alternate briefs employees on the sensitivity of CNWDI prior to their having access to CNWDI information.</p> <p>Debriefings: When the employee terminates access to CNWDI, give him or her an oral debriefing that includes:</p> <ul style="list-style-type: none"> • Purpose of the debriefing. • Serious nature of the subject matter which requires protection in the national interest. • Need for caution and discretion. 	<p>The abbreviation CNWDI (pronounced SIN-widdy) stands for "Critical Nuclear Weapons Design Information". NISPOM, Chapter 9, Section 2 details the requirements that apply to CNWDI. The briefing that you give employees must include the following: Definition of CNWDI. Reminder of the extreme sensitivity of CNWDI.</p> <ul style="list-style-type: none"> • Explanation of the individual's continuing responsibility for properly safeguarding CNWDI and for ensuring that dissemination is strictly limited to other personnel who have been authorized for access and have a need-to-know for the particular information. • Any special local requirement • Retain record 2 yrs following termination
<p>NATO Briefing</p>	<p>NISPOM, 10-705</p>	<p>Briefing of FSO: A US Government representative will give the FSO an initial NATO briefing.</p> <p>Employee Briefings: The FSO provides an initial NATO briefing to employees prior to having access to NATO information.</p> <p>Refresher Briefings: Conduct annual refresher briefings for all employees who have access to NATO information.</p> <p>Debriefings: When an employee no longer requires access to such information, debrief the employee.</p>	<p>The term "NATO classified information" circulated within and by the member countries of the North Atlantic Treaty Organization (NATO). It includes information released by member nations into the NATO security system, as well as information originating within NATO. The NISPOM, Chapter 10 prescribes the special requirements for marking, handling, and safeguard NATO materials. The briefing that you give employees must cover applicable NATO security procedures and "the consequences of negligent handling." Have the employees sign a certificate stating that they have been briefed (or debriefed) and acknowledge their responsibility for safeguarding NATO information. Such certificates shall be maintained 2 years for access to NATO SECRET, CONFIDENTIAL and RESTRICTED. Certificates for access to COSMIC TOP SECRET and all ATOMAL information shall be maintained for 3 years.</p>

SPECIAL BRIEFINGS - 2

Type	Reference	When to Give	Comments
<p>COMSEC Information Briefing</p>	<p>National Security Agency (NSA) Industrial COMSEC Manual (NSA Manual 90-1) "Annex A"</p>	<p>The facility's DSS Representative or a US government representative will give the FSO an initial COMSEC briefing.</p> <p>Briefing of Employees: The FSO provides required briefings and training to the COMSEC custodian and other employees who have access to COMSEC information.</p>	<p>COMSEC stands for "Communication Security" and refers to the steps taken to protect information of intelligence value when it is being telecommunicated. If your firm is involved with COMSEC, then you or the COMSEC custodian or alternate custodian must brief the other employees at your facility regarding COMSEC. Base the briefing on Annex A of the NSA Industrial COMSEC manual (NSA Manual 90-1)</p>

SUMMARY

Briefings are an important part of a facility security education program. Many firms give all employees an initial company briefing, though the NISPOM does not require it. The initial security briefing must be given to all cleared employees before permitting them access to classified information. This briefing introduces them to the US government's Information Security Program and to the requirements imposed on User Agencies and their contractors. The briefing also informs them of their obligation regarding classified information and of the security procedures they are to follow. Following this briefing, employees execute the Classified Information Nondisclosure Agreement, SF 312, to certify awareness of their obligations. Employees must be given refresher briefings periodically. To ensure that a cleared employee is aware of his or her continuing responsibility to protect classified information, debrief the employee when the employee's service terminates; when the employee's PCL is terminated, suspended, or revoked; and upon termination of the FCL.

8 - Review Exercises

Complete the following exercises for review and practice.

Multiple-choice questions may have one or more correct choices.



1. Write "ICB" beside the items below that describe an *initial company briefing*. Write "ISB" beside the items that describe an *initial security briefing*.

_____ Tailored to the security procedures associated with a specific job.

_____ Usually given to both cleared and uncleared employees.

_____ Given to all cleared employees before permitting them access to classified information.

_____ Not required by NISPOM.

_____ Followed by execution of SF 312.

2. A cleared employee's responsibilities in safeguarding classified information include

() a. not communicating classified information to an unauthorized person or agency.

() b. making original classification decisions.

() c. determining whether a prospective recipient of classified information is an authorized person.

() d. advising the person to whom the employee has disclosed classified information of its classification level.

3. The contents of an *initial security briefing* include which of the following?
- () a. Security procedures and duties applicable to the employee's job.
 - () b. Employee reporting obligations and requirements.
 - () c. Threat Awareness Briefing.
 - () d. Overview of the security classification system.
 - () e. Defensive Security Briefing.
 - () f. Execution of DD Form 254, DoD Contract Security Classification Specification.
4. Refresher training must *at least*
- a. Be provided a _____ to all cleared employees.
 - b. R_____ information presented during the initial security briefing,
 - c. Inform employees of appropriate c_____ in security regulations.
 - d. Maintain suitable r_____ about the programs offered and employee participation in them.
5. Which of the following are true of SF 312?
- () a. It is a legal document.
 - () b. By signing it, the employees certify that they are aware of their obligations regarding classified information and of the penalties for violating these obligations.
 - () c. The FSO signs it.
 - () d. The FSO sends the form to DISCO after the employee has received the initial security briefing.
 - () e. The FSO must submit a report to DISCO if an employee refuses to sign it.

6. The purpose of the security debriefing is to formally release cleared employees from their obligations regarding classified information.

() True. () False.

7. Under which of the following circumstances must the security debriefing be given to a cleared employee?

() a. The employee's periodic re-investigation report was forwarded to DOHA (Defense Office of Hearings and Appeals).

() b. The employee terminates employment with your firm.

() c. The employee is assigned to a different facility operated by your company.

() d. Your facility's FCL is terminated.

() e. The employee's PCL is terminated, suspended, or revoked.

8. You will recall that Avery Ivory, the widget designer at EWC, held a TOP SECRET clearance at the time of his retirement. What actions did EWC's FSO Harold Huxtable take when Mr. Ivory retired?

8 - Solutions & References



1. ISB Tailored to the security procedures associated with a specific job. (p. 8-2 to 8-9).
ICB Usually given to both cleared and uncleared employees. (p. 8-2).
ISB Given to all cleared employees before permitting them access to classified information. (p. 8-2).
ICB Not required by NISPOM. (p. 8-2).
ISB Followed by execution of SF 312. (p. 8-9).
2. a., c., d. (pp. 8-3 to 8-9).
3. a., b., c., d., e. (pp. 8-2 to 8-9).
4. a. annually.
b. Reinforce.
c. changes.
d. records. (pp. 8-10 & 8-11).
5. a., b., c., d., and e. (p. 8-9 & 8-10).
6. False. (p. 8-11).
7. b., d., e. (p. 8-11).
8. Harold gave Mr. Ivory a security debriefing. Then Harold completed a DISCO Form 562 and sent it to DISCO. (p. 8-11).