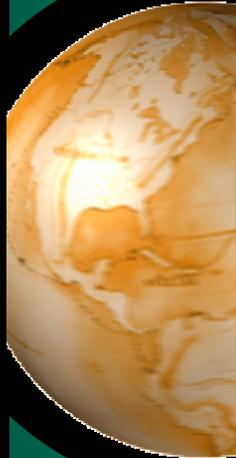


# Basic Industrial Security For User Agency Personnel

IS001.8 Revision 1



# Preface

We have made every effort to ensure that the contents of this course are in accord with all applicable policies in effect at the time it was reviewed for publication. However, such policies may change in the interval between reviews, and the technical accuracy of a given edition of the sub-course cannot be guaranteed in all particulars. Questions regarding technical accuracy should be directed to your DSS Field Office. However, you should base your responses to the questions in the course examination solely on the information provided in the course and not on any other source.

# Definitions

For the purpose of this course it is necessary to define the following two terms:

**Government Contracting Activity - GCA** - An element of an agency designated by the agency head and delegated broad authority regarding acquisition functions.

**User Agency (UA)** - As a general rule, this term as used throughout this course refers to all government agencies that operate under the rules of the NISP. However, in some situations a distinction must be made and the terms DoD User Agency, non-DoD User Agency and non-User Agency are used as needed. The term, DoD User Agency, refers to the OSD (including all boards, councils, staffs, and commands), DoD agencies and the Departments of the Army, Navy and Air Force (including all their activities). The term non-DoD User Agency refers to the Departments of State, Commerce, Treasury, Transportation, Interior, Agriculture, Labor and Justice, and the NASA, GSA, SBA, NSF, EPA, ACDA, FEMA, GAO, FRS, USIA, USTR and USITC. The term non-user agency refers to all other government agencies that do not participate in the NISP to include Health and Human Services and the Department of Education at the present time.

In the NISP the terms are almost interchangeable but there are some subtle distinctions. For the most part the Government Contracting Activity is that entity designated by an agency to award contracts for goods and services needed by the government. The User Agency is that part of an organization that has agreed to protect classified information under the rules of the NISP and includes all segments of the organization not just the contracting portion.

October 2002

# Acronyms & Abbreviations

ACDA	U.S. Arms Control and Disarmament Agency
AIS	Automated Information System
CAGE	Commercial and Government Entity Number
CIA	Central Intelligence Agency
CM	Classification Management
COMSEC	Communications Security
CSA	Cognizant Security Agency
CSO	Cognizant Security Office
CVA	Central Verification Activity
DCII	Defense Clearance and Investigations Index
DCMC	Defense Contract Management Command
DSS	Defense Security Service
DISCO	Defense Industrial Security Clearance Office
DOB	Date of Birth
DoD	Department of Defense
DSSA	Defense Security Service Academy
DOHA	Defense Office of Hearings and Appeals
E.O.	Executive Order
FBI	Federal Bureau of Investigation
FCIL	Facility Security Clearance
FMS	Foreign Military Sales
FNAC	Facility National Agency Check
FOCI	Foreign Ownership, Control, or Influence
GCA	Government Contracting Activity
GFE	Government Furnished Equipment
GSOMIA	General Security of Military Information Agreement
IFB	Invitation for Bids
INS	Immigration and Naturalization Service
ISOO	Industrial Security Oversight Office
ISR	Industrial Security Regulation
I.S. Rep	Industrial Security Representative
KMP	Key Management Personnel
LAA	Limited Access Authorization
LAC	Local Agency Check
LOC	Letter of Consent
MAP	Mutual Aid Program
MFO	Multiple Facility Organization
MPRC	Military Personnel Records Center
NAC	National Agency Check
NATO	North Atlantic Treaty Organization
NISP	National Industrial Security Program
NISPOM	National Industrial Security Program Operating Manual
NSD	National Security Directive
OADR	Originating Agency's Determination Required
OSSI	Office of Security Services International

OPM	Office of Personnel Management
OSD	Office of the Secretary of Defense
PIC	Personnel Investigations Center
POB	Place of Birth
POI	Period of Investigation
PR	Periodic Reinvestigation
RF	Radio Frequency
RFP	Request for Proposals
RFQ	Request for Quotes
ROI	Report of Investigation
SSBI	Single Scope Background Investigation
SCI	Sensitive Compartmented Information
SPP	Standard Practice Procedures
SOR	Statement of Reasons
SOW	Statement of Work
UA	User Agency
U.S.	United States

# TABLE OF CONTENTS

	Page Number
<b>Preface</b>	i
<b>Definitions</b>	ii
<b>Acronyms and Abbreviations</b>	iii
<b>Table of Contents</b>	v
<b>LESSON 1. THE FACILITY SECURITY CLEARANCE</b>	1-1
<b>LESSON 2. PERSONNEL SECURITY CLEARANCES</b>	2-1
<b>LESSON 3. VISITOR CONTROL</b>	3-1
<b>LESSON 4. CLASSIFICATION MANAGEMENT</b>	4-1
<b>LESSON 5. SAFEGUARDING CLASSIFIED INFORMATION</b>	5-1
<b>LESSON 6. VIOLATIONS AND COMPROMISES</b>	6-1
<b>LESSON 7. INTERNATIONAL ACTIVITIES</b>	7-1
<b>LESSON 8. INFORMATION SYSTEMS SECURITY</b>	8-1
<b>LESSON 9. REVIEWS</b>	9-1
<b>EXAMINATION</b>	E-1
<b>INDEX</b>	vi

## LESSON 1

# The Facility Security Clearance

With limited exceptions, the U.S. Government does not own or directly control our nation's research, development, production, or service facilities that support the national defense effort. And so, when acquiring weapons and defense systems or services, the Government must turn to private industry. To fulfill its role, private industry often requires access to or possession of classified defense information.

The controls and procedures implemented under the National Industrial Security Program (NISP) for the protection of classified information depend in large part on personnel, information, and physical security controls. However, in recognition of the nature of private industry and its inherent structures which control and influence the organization, the NISP incorporates a fourth facet into its system: the facility clearance concept. It makes sense to start you out with this concept, for without a valid facility security clearance at the appropriate level, a contractor cannot be furnished classified information nor can its employees be afforded access to classified information.

In this lesson, besides explaining the facility security clearance concept, we will provide a few definitions associated with it and then discuss the six essential elements of a facility security clearance. We will also point out those changes at the facility that may affect its clearance and must, therefore, be reported. We will go over administrative termination and reinstatement of a facility clearance, then well wind up with a look at the two ways in which a cleared contractor may be constituted on a User Agency installation.

## OBJECTIVES

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

- Define "Facility Security Clearance" (FCL).
- Recall the definitions of "access" and "classified contract."
- Recall key aspects of the five essential elements of a FCL.
- State the main concern of the Defense Security Service (DSS) when a change affecting the basis for granting the facility clearance occurs at a facility.
- State the circumstances under which the DSS will administratively terminate a facility security clearance.
- Differentiate the roles of the DSS and the installation commander when a contractor facility is located on the military installation.

## **“FACILITY” DEFINED**

Before discussing facility security clearances, we need to be sure that we have a clear understanding of what the term "facility" means within the NISP. Quite simply, a facility is a plant, office, college, associated warehouses, or components which, when related by function and location, form an operating entity. Facilities range in size from the huge corporate complex to the small one-person office.

## **THE FACILITY SECURITY CLEARANCE CONCEPT**

DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), defines "Facility Security Clearance" as "an administrative determination that, from a security viewpoint, a facility is eligible for access to classified information of a certain category (and all lower categories)." Note these two key points:

- A clearance is an administrative determination made by the Government, specifically by the Industrial Security Representative (IS Rep), in making a decision regarding a contractor's eligibility for a facility clearance. The IS Rep focuses on the information collected and evaluated during the survey(s) conducted for a Facility Security Clearance (FCL).
- Based on the IS Rep's favorable determination, the Defense Industrial Security Clearance Office (DISCO), a division of the Defense Security Service (DSS) issues the FCL.
- You need to know two more definitions because a facility security clearance is granted only when there is a requirement for a facility to have access to classified information in the performance of a classified contract.

**Access:** The ability and opportunity to gain knowledge of the classified information. Always keep in mind the fact that an individual could gain access by seeing, hearing, or touching classified information/hardware. It doesn't always involve taking physical possession of the classified information.

**Classified Contract:** Any contract which requires the employees to have access to classified information in order to provide the product or service. This doesn't mean the contract document is itself classified.

## **FIVE ESSENTIAL ELEMENTS**

The administrative determination that a facility is eligible for access to classified information is based on five considerations, which can be referred to as the "Five Essential Elements." These elements are as follows:

- **Sponsorship**
- **Security Agreement**
- **Certificate Pertaining to Foreign Interests**
- **Organization**
- **KMP clearances**

A facility must satisfy the established requirements in all five of these areas to be granted a clearance.

## **SPONSORSHIP**

Sponsorship is an essential element of a facility security clearance because it is the means of identifying those contractors who have a need for access to classified information. A contractor cannot request that his or her facility be cleared. Sponsorship begins when, in addition to the need for a supply or service by the Government Contracting Activity (GCA) that initiates the acquisition cycle, there is also a need for the contractor or his/her employees (and perhaps his/her subcontractors and their employees) to have a need to access to classified information in order to supply that supply or service. Prospective contractors cannot prepare their bids or proposals without having a clear understanding of what will be required. They may require access to prepare their bids or proposals (often they do not need such access even though contract performance will require access).

In order to have access, they must first be cleared as a facility. Since prospective contractors cannot sponsor themselves, the User Agency, as the requiring activity, must identify as part of the solicitation process, prospective prime contractors who will require access at a certain level to: 1. Prepare their bids or proposals, and/or 2. Perform under the classified contract when it is awarded. These prime contractors, once they have been cleared, may in turn identify subcontractors who will require access for pre-contract and/or contract performance purposes. If it is determined that all of these prime contractors and subcontractors already have valid facility clearances at the proper level or higher, no further sponsorship is required. This determination is made by contacting DSS Central Verification Activity (DSS-CVA) at (888) 282-7682. If any do not have valid FCLs, then the User Agency or a cleared contractor must sponsor the uncleared contractors or subcontractors.

Specifically, sponsorship consists of the cleared contractor or User Agency requesting in writing that DISCO initiate facility clearance action. The request should identify the facility to be cleared, define the classified acquisition need requiring the clearance action, and state the level of clearance and any storage requirements. All facility security clearances are issued on an interim basis at the SECRET level if the facility is eligible.

There are thus three main considerations with sponsorship:

- There must be a bonafide classified acquisition need.
- A contractor cannot sponsor himself/herself for a facility security clearance.
- Only a User Agency or a cleared contractor or subcontractor can sponsor a contractor for a clearance. Remember, too, that this process of clearing the facility may be time consuming. Allow as much lead-time as possible when sending in a facility clearance request.

Another essential element of a facility security clearance is the execution of the Security Agreement (DD Form 441). The agreement is signed and becomes part of the contract documents. There are six sections to this form, and we will discuss each of them in what follows.

You will see that one of the things the contractor agrees to do by signing this form is to utilize the National Industrial Security Program Operating Manual (NISPOM). The NISPOM provides the guidance necessary for contractors to establish a security program which will protect the classified information and materials to which they have access. This is done using risk management principles and with the assistance of the IS Rep.

Now let's turn to a discussion of the six sections to the Security Agreement.

## **SECURITY AGREEMENT**

**Section I - SECURITY CONTROLS.** This section stresses that it is the NISPOM that provides contractors the guidance they need to set up effective security programs. Specifically, the contractor agrees to "provide and maintain a system of security controls within its or his own organization" in accordance with NISPOM requirements. Note that it is mainly up to the contractor to implement and monitor security measures at the facility. Note also that the NISPOM becomes part of the contract. If the NISPOM is revised, the contractor needs to implement the revision. In exceptional situations the parties may, by mutual agreements (waivers), adapt the NISPOM to any special requirements of the contractor's business. The second main contractor obligation is, if determined necessary by the facility security officer or the IS Rep, to prepare written Standard Practice Procedures (SPP) which are consistent with the NISPOM. Finally, skipping to paragraph (C), the contractor agrees to determine that any subcontractor, vendor, or supplier who will require access to classified information has its own facility security clearance. Under Section I, then, the contractor agrees to do quite a lot (with Government guidance).

What does the Government in turn agree to do? The Government's primary responsibilities here are in two areas: classification guidance and personnel security clearances. The Government will give the contractor written notice of what needs to be protected and to what degree (i.e., classification guidance). Further, the Government will assign the least restrictive classification, since "over classification causes unnecessary operational delays and depreciates the importance of correctly classified matter." Finally, the Government agrees to process the contractor's employees for appropriate personnel clearances, as required.

**Section II - INSPECTION.** One of the responsibilities of the DSS is to provide assurance to the GCA that the contractor is protecting their classified information. One basis for this assurance is the periodic security reviews that DSS conducts. Events which would require that DSS conduct a more frequent review could include new counterintelligence information indicating a new or increased threat to the facility or its technologies, changes in the scope of the facility's classified operations, the departure of the facility security officer (FSO), major or repeated security violations indicating classified information is in jeopardy, the introduction of foreign ownership, control, or influence (FOCI) or significant changes to current FOCI, foreign nationals visiting or assigned to the facility, and significant international involvement, to name a few. This section of the agreement establishes the Government's right to conduct these reviews.

**Section III - MODIFICATION.** As with most contracts, the Security Agreement does provide for modification in exceptional circumstances. However, this is seldom, if ever, done.

**Section IV - TERMINATION.** Either party can terminate the Security Agreement by giving the other party a 30-day written notice. The important point here is that even though the agreement is terminated, the contractor is obligated to protect any classified information in his/her possession or under his/her control as if the agreement had not been terminated. (This includes classified information in his/her head.)

**Section V - PRIOR SECURITY AGREEMENTS.** This section simply establishes that whatever such agreements the contractor may have signed in the past, and whatever may have been said to him/her about the subject matter of the Security Agreement in the past, the only thing that counts now is this Security Agreement. This section does not, however, nullify any special security clauses that a User Agency may have included or may elect to include in its classified contracts. (These special security clauses should never countermand or weaken the provisions of the Security Agreement or of the NISPOM, but should instead serve only to supplement them.)

**Section VI - SECURITY COSTS.** This section means that this agreement does not obligate the Government to pay for the contractor's costs in establishing security controls (e.g., buying security containers, constructing controlled areas, taking the necessary time to process individuals for clearances, preparing the SPP, etc.). It basically means that security costs should be included in the response to the Invitation for Bid (IFB) or Request for Proposal (RFP) with the contractor's other costs to provide the required supply or service. Security costs which may arise over and above the price of the awarded contract must be agreed to in writing by the contracting officer (or designated representative) before the Government is obligated to reimburse the contractor for them.

## **CERTIFICATE PERTAINING TO FOREIGN INTERESTS**

Concurrently with the execution of the Security Agreement (DD Form 441), the facility must execute the Certificate Pertaining to Foreign Interests (SF 328). If the facility is a subsidiary, the parent must also execute a SF 328. The importance of this form is that it is one of several means in the identification and assessment of the sources of power that affect the facility, in this case, to determine if these sources of power are foreign interests or are influenced by foreign interests. The general policy is that a facility which is determined to be under Foreign Ownership, Control, or Influence (FOCI) is ineligible for a facility security clearance (except where the FOCI stems from certain nations allied with the U.S. with whom we have entered into "Limited Industrial Security Agreements").

When is a facility determined to be under FOCI? According to the NISPOM, "a U.S. company is considered under FOCI whenever a foreign interest has the power, direct or indirect, whether or not exercised, and whether or not exercisable through the ownership of the U.S. company's securities, by contractual arrangements or other means, to direct or decide matters affecting the management or operations of that company in a manner

which may result in unauthorized access to classified information or may affect adversely the performance of classified contracts."

Since the SF 328 is the key document in the determination of FOCI, we'll briefly address its main points. Like the Security Agreement, the Certificate Pertaining to Foreign Interests is a concise, two-page document. The areas covered by the 11 questions it asks may be summarized as follows:

- Foreign ownership of the organization.
- Organization ownership of foreign interests.
- Ability of foreign interests to control or influence organization management.
- Organization contracts with foreign interest.
- Organization indebtedness to foreign interests.
- Organization income from foreign interests.
- Possible foreign investment in organization.
- Organization linked by management to foreign interest.
- Potential foreign interest access to classified information at facility.
- Other foreign interest involvement with organization.

Note that "a U.S. company determined to be under FOCI is ineligible for an FCL, or an existing FCL shall be suspended or revoked unless security measures are taken as necessary to remove the possibility of unauthorized access or the adverse affect on classified contracts." DSS wants to be assured that the contractor is not coerced into disclosing classified information.

## **ORGANIZATION**

While the identification and assessment of foreign ownership, control, and influence (FOCI) is essential in determining a facility's suitability for access, the identification and assessment of its domestic ownership and its resulting control and influence is an equally important element. In the area of organization, this means that we need to identify and assess any other facilities that by their relationship to the facility in question, may control or influence its protection of classified information. First, though, let's state the Multiple Facility Organization (MFO) together comprise a single legal entity, only the home office facility can normally execute a Security Agreement (DD Form 441) with the government. As required, subordinate facilities (divisions) can be included in and covered by the provisions of the home office facility's Security Agreement by the execution of an appendage to the Security Agreement (DD Form 441-1). As noted, a separate facility security clearance action is required for each facility on the DD Form 441-1. The SF 328 is not required of a division.

## **THE PARENT-SUBSIDIARY RELATIONSHIP**

Since, by definition, a subsidiary is controlled by its parent (by the parent's ownership of a majority of the subsidiary's stock), the guideline is that the parent must have a facility security clearance of the same or higher level than the subsidiary. However, the parent-subsubsidiary relationship differs in an important way from the MFO, and the NISP has taken

this difference into account in its regulations. Unlike the MFO, where we are dealing with a single legal entity, in a parent-subsidary relationship the parent and each of its subsidiaries are separate legal entities. Since a subsidiary is thus legally accountable in its own right, the NISP permits the parent to remain uncleared or a subsidiary to be cleared at a higher level than its parent does. In such cases the parent must first submit a Certificate Pertaining to Foreign Interests. DSS is concerned about any foreign involvement by the parent company. Should FOCl be a factor, the subsidiary would not be eligible to be cleared until the FOCl was mitigated. Then the Board of Directors of the parent formally excludes the parent from access to either: 1. All classified information held by the subsidiary, or 2. Classified information held by the subsidiary, which is of a higher level than the general rule. Each facility is considered to be a separate entity and as such, it requires its own facility clearance. However, there are two cases in which, though the facility still requires its own clearance, the clearance status of other facilities related to it is an issue. These two situations are the multiple facility organization and the parent-subsidary relationship. It is important to bear in mind that although we will discuss these two situations as separate cases, there are in fact many instances where both relationships are combined within a single business. Such a combination of relationships, as when a subsidiary is also the home office of a multiple facility organization, does not, however, alter the application of the general guidelines described below.

## **THE MULTIPLE FACILITY ORGANIZATION**

Any of the business structures you may have studied, either sole proprietorships, partnerships, corporations, colleges and/or universities, may be configured (organized) as a multiple facility organization (MFO), i.e., a legal entity which is composed of two or more facilities. The guideline when clearing any subordinate facility of a MFO is quite simple; the home office facility (HOF) must have a facility security clearance of the same or higher level than the subordinate facility. The reason for this is also quite simple. The other facilities (divisions, branch offices, etc.) of the MFO are subordinate to the home office facility, and their operations are usually quite closely linked. Accordingly, if the home office were not cleared at the same or higher level, then the home office could have unauthorized access to the classified information available to a subordinate facility (division). We are also concerned with the amount of control and influence the home office has over its branch offices. It is important to note that since all of the facilities of a level of the parent's facility security clearance. The subsidiary must then ensure that the parent is indeed denied access to higher-level classified information.

## **KEY MANAGEMENT PERSONNEL CLEARANCE**

In this element, we are concerned with identifying and assessing other sources of power affecting control of the facility: the facility's Key Management Personnel (KMPs). The NISPOM states that "the senior management official and the FSO must always be cleared to the level of the FCL." In addition, the NISPOM recognizes that there are others within an organization who can control or influence management decisions. Accordingly, the NISPOM goes on to state that "other officials, as determined by [DSS], must be granted a

PCL or be excluded from classified access." It is therefore essential that the facility's KMPs be identified and individually cleared, even if they are not going to have "hands-on" access to classified information. (Again, certain KMPs may be permitted to be excluded from this personnel security clearance requirement.) In recognition of the differences among the various business structures, DSS has established the categories of KMPs requiring personnel clearances that are often appropriate for the particular structure.

Prior to any other clearance actions, the "List of Parties Excluded From Federal Procurement or Non-Procurement Programs" prepared by the General Services Administration is also checked by DISCO to determine whether a contractor has been placed on the list and the reason for the placement.

## **FACILITY SECURITY CLEARANCE NOTIFICATION LETTER**

Only when the facility has successfully fulfilled these five essential elements:

- When it has been properly sponsored;
- When it has executed a Security Agreement;
- When, if applicable, its home office or parent has been properly cleared or, if allowed, excluded;
- When it has been determined not to be under FOCI; and
- When its KMPs have been properly cleared or, if allowed, excluded.

Only then does DSS issue the facility a Letter of Notification of Facility Security Clearance (DSS FL 381R).

## **CHANGED CONDITIONS**

Even though a facility has been issued a facility security clearance there are certain things which could affect its continuation in the NISP. The first consideration on the part of DSS, regardless of the nature of the change, is the continued protection of the classified information. Some of the changes which could result in the invalidation of the FCL would be:

- Change in ownership or management.
- Change in operating name.
- Change in address.
- Closing of the business.
- Change in KMPs.
- Change in FOCI information.

As you can see, these changes require some type of action on the part of the facility to revalidate its facility security clearance. Contractors are required to report these changes to the DSS Field Office as soon as they are known in order that appropriate action may be initiated to ensure the continuance of the FCL.

As a general rule a facility may remain in the NISP for as long as there is a GCA acquisition need that requires the facility to have access to classified information. If, however, a facility no longer requires access or has access merely because it has been authorized to retain classified information after completing a classified contract, DSS will allow the facility to remain in a "dormant" status for a period of 18 months. If the facility has no need for its clearance during this period, DSS will terminate the clearance.

## **REPROCESSING**

Should a facility, after its FCL is administratively terminated, again require access to classified information, the DSS can reinstate the FCL if it was terminated within the preceding 24 months and there have been no changes which could otherwise invalidate the FCL. After the IS Rep conducts a survey of the facility to ensure that there are no changed conditions, DSS simply reinstates the FCL and all employee clearances. If, however, it has been longer than 24 months, the whole administrative determination process must be accomplished once more.

## **FACILITIES ON USER AGENCY INSTALLATIONS**

The Industrial Security Regulation (DoD 5220.22-R) designates the Defense Security Service (DSS) to administer the NISP. This administration is ultimately carried out through the various DSS Field Offices. Only DSS can grant facility security clearances. But what about those cleared contractors located on User Agency installations? Normally these contractors fall into two main categories, cleared facilities and visitor groups.

**Cleared Facilities:** If the visitors control their site on the installation, have a semi-permanent operation, and maintain their own security controls, then, if the installation commander wishes them to be cleared as a facility, the facility will be cleared by DSS. The on-site survey may be accomplished by either a DSS IS Representative or a User Agency IS Representative, but in either case it is DSS, through DISCO, that issues the facility clearance. The installation commander must decide whether to have DSS conduct reviews of the facility or to have the installation security personnel conduct them.

**Visitor Groups:** If the visitors do not control their site on the installation, have a semi-permanent operation, and maintain their own security controls, or if the installation commander does not want them cleared as a facility, then they will be treated as a visitor group. The installation will enter into a "Visitor Group Agreement," which spells out the security controls that the visitors will apply while performing on the installation. Paragraph 1-108 of the Industrial Security Regulation details these procedures. The installation security personnel, utilizing the agreement, inspects the group.

## **SUMMARY**

A contractor's participation in the NISP is based on the facility security clearance concept. Classified information may be accessed by a contractor only when there is a valid facility security clearance, need-to-know, and when appropriate, adequate safeguarding capability to support the access requirement. Issuance of an FCL is based upon five essential

elements. Certain changed conditions may affect the status of the FCL. A dormant facility's FCL will be administratively terminated, but if access is again required the FCL can be reinstated. A cleared contractor located on a UA installation may be constituted as a cleared facility or a visitor group.

## REVIEW EXERCISES

Complete the following exercises for review and practice.

1. A facility security clearance is an administrative determination made by the Industrial Security Representative. The FCL is issued by the Defense Industrial Security Clearance Office.  
S \_\_\_\_\_  
C \_\_\_\_\_ O \_\_\_\_\_.
2. Access is defined within the NISP as "the ability and opportunity to obtain knowledge of classified information."  
  
True  
False
3. A classified contract is any contract which requires the employee(s) to have a \_\_\_\_\_ to classified information in order to provide the product or service.
4. To be eligible for an FCL, a contractor must be sponsored by another cleared contractor \_\_\_\_\_ or by a User Agency \_\_\_\_\_.
5. The DD Form 441 (Security Agreement) calls for the contractor to establish a sound security program based on the guidance in the National Industrial Security Program Order \_\_\_\_\_ Manual \_\_\_\_\_.
6. If a facility is a subsidiary, the parent must also execute a Certificate of Protection \_\_\_\_\_ to Facility \_\_\_\_\_ Information \_\_\_\_\_.
7. For a Multiple Facility Organization (MFO) to be cleared, the Headquarters \_\_\_\_\_ Office \_\_\_\_\_ Facility \_\_\_\_\_ must have a facility clearance at the same level as, or a higher level than, any of its cleared divisional offices.
8. When changed conditions occur at a cleared facility the first consideration of the DSS is the facility's continued ability to protect \_\_\_\_\_ control \_\_\_\_\_ information \_\_\_\_\_.
9. DSS will administratively terminate the FCL of a facility that has been downgraded for \_\_\_\_\_ months.
10. If a User Agency installation commander desires a cleared contractor located on the installation to be considered for an FCL, the FCL will be issued by DSS.

True  
False

# ANSWERS

## Solutions and References

1. *Security Clearance Office (p. 1-2)*
2. *True (p. 1-2)*
3. *access (p. 1-2)*
4. *contractor*  
*User Agency (p. 1-3)*
5. *Operating Manual (p. 1-4)*
6. *Pertaining to Foreign Interests (p. 1-6)*
7. *Home Office Facility (p. 1-7)*
8. *protect classified information (p. 1- 8)*
9. *dormant, 18 (p. 1-8)*
10. *True (p. 1-9)*

## LESSON 2

# Personnel Security Clearances

The success or failure of the NISP depends largely upon the individuals who are responsible for the proper safeguarding and handling of the classified information entrusted to them. It is essential that industrial personnel requiring access to classified information be eligible and trustworthy. The Industrial Personnel Security Clearance Program establishes a means whereby the government can determine if an individual possesses the necessary trustworthiness and integrity to enable that person to have access, and whether such access is clearly consistent with the national interest.

While the program aims to prevent penetrations of the Department of Defense by hostile intelligence, the most tangible results are to grant security clearances to persons whose past actions have indicated that they are reliable, stable, law-abiding, and free from factors that would make them vulnerable to approach by hostile intelligence, and to deny clearances to those who do not meet these criteria. It must be remembered that the granting of a clearance, either military or within industry, is a calculated risk, based on the findings of the investigation of the individual.

## OBJECTIVES

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

- Explain the clearance and adjudicative processes used for industry.
- Identify the types of personnel security investigations conducted on industrial personnel.
- Explain the use and purpose of Limited Access Authorizations.
- Identify the various Agency responsibilities in different clearance procedures.

## IMPORTANCE OF A PERSONNEL SECURITY CLEARANCE

A personnel security clearance is an administrative determination or prediction that an individual can be relied on to safeguard our national secrets. Why is a personnel security clearance important?

First, every security clearance is important to our country. Our national survival depends in part upon the ability of the United States to maintain technological superiority over potential enemies. To accomplish this goal, we must be able to entrust our state secrets to personnel who will safeguard them.

From another perspective, personnel security clearances are important to DoD contractors because having appropriately cleared employees is a prerequisite to the contractors' being eligible to perform on classified contracts.

In like manner, holding a security clearance is important to the individual employee. Having the clearance and a "need-to-know" for access to certain national security information makes that employee an "authorized person" permitted to deal with the classified information necessary to do the job.

## **CLEARANCE ELIGIBILITY CRITERIA**

The NISPOM defines a personnel security clearance as "an administrative determination that an individual is eligible, from a security point of view, for access to classified information of the same or lower category as the level of the personnel clearance being granted." This determination is based on investigation designed to gather, uncover, and develop information bearing on the individual's involvement with 13 eligibility criteria. Note that under the NISPOM there are no longer any minimum age requirements for the various clearances.

### **PERSONNEL SECURITY CLEARANCE ELIGIBILITY CRITERIA**

**IDEALLY, A PERSON SHOULD NOT HAVE A HISTORY OF ANY OF THE FOLLOWING 13 ACTIVITIES AND CONDITIONS, ALTHOUGH A PARTICULAR "INVOLVEMENT" WILL NOT NECESSARILY IN AND OF ITSELF BE A BASIS FOR A DENIAL OF CLEARANCE.**

**a. Guideline A: Allegiance to the United States.**

*The Concern.* An individual must be of unquestioned allegiance to the United States, the willingness to safeguard classified information is in doubt if there is any reason to suspect an individual's allegiance to the United States.

**b. Guideline B: Foreign Influence**

*The Concern;* A security risk may exist when an individual's immediate family, including cohabitants and other persons to whom he or she may be bound by affection, influence, or obligations are not citizens of the United States or may be subject to duress. These situations could create the potential for foreign influence that could result in the compromise of classified information. Contracts with citizens of other countries or financial interests in other countries are also relevant to security determinations if they make an individual potentially vulnerable to coercion, exploitation, or pressure.

**c. Guideline C: Foreign Preference**

*The Concern:* When an individual acts in such a way as to indicate a preference for a foreign country over the United States, then he or she may be prone to provide information or make decisions that are harmful to the interests of the United States.

**d. Guideline D: Sexual Behavior**

*The Concern:* Sexual behavior is a security concern if it involves a criminal offense, indicates a personality or emotional disorder, may subject the individual to coercion, exploitation, or duress, or reflects lack of judgement or discretion. Sexual orientation or preference may not be used as a basis for or a disqualifying factor in determining a person's eligibility for a security clearance.

**e. Guideline E: Personal Conduct**

*The Concern:* Conduct involving questionable judgment, untrustworthiness,

unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information. The following will normally result in an unfavorable clearance action or administrative termination of further processing for clearance eligibility:

**f. Guideline F: Financial Considerations**

*The Concern:* An individual who is financially overextended is at risk of having to engage in illegal acts to generate funds. Unexplained affluence is often linked to proceeds from financially profitable criminal acts.

**g. Guideline G: Alcohol Consumption**

*The Concern:* Excessive alcohol consumption often leads to the exercise of questionable judgment, unreliability, failure to control impulses, and increases the risk of unauthorized disclosure of classified information due to carelessness.

**h. Guideline H: Drug involvement**

*The Concern:* Improper or illegal involvement with drugs raises questions regarding an individual's willingness or ability to protect classified information. Drug abuse or dependence may impair social or occupational functioning, increasing the risk of an unauthorized disclosure of classified information.

**i. Guideline I: Emotional, mental, and personality disorders.**

*The Concern:* Emotional, mental, and personality disorders can cause a significant deficit in an individual's psychological, social and occupational functioning. These disorders are of security concern because they may indicate a defect in judgment,

reliability, or stability. A credentialed mental health professional (e.g., clinical psychologist or psychiatrist), employed by, acceptable to or approved by the government, should be utilized in evaluating potentially disqualifying and mitigating information fully and properly, and particularly for consultation with the individual's mental health care provider.

**j. Guideline J: Criminal Conduct**

*The Concern:* A history or pattern of criminal activity creates doubt about a person's judgment, reliability and trustworthiness.

**k. Guideline K: Security Violations**

*The Concern:* Noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information.

**l. Guideline L: Outside Activities**

*The Concern:* Involvement in certain types of activities outside employment or activities of security concern if it poses a conflict with an individual's security responsibilities and could create an increased risk of unauthorized disclosure of classified information.

**m. Guideline M: Misuse of Information Technology Systems**

*The Concern:* Noncompliance with rules, procedures, guidelines, or regulations pertaining to information technology systems may raise security concerns about an individual's trustworthiness, willingness, and ability to properly protect classified systems, networks, and information. Information Technology Systems include all related equipment used for the communication, transmission, processing, manipulation, and storage of classified or sensitive information.

## **TYPES OF INDUSTRIAL CLEARANCES**

In most cases, industrial personnel are granted final clearances at one of the three basic levels: CONFIDENTIAL, SECRET, or TOP SECRET. Such clearances may be initial (first-time) clearances or reinstated industrial clearances, or non-industrial (i.e., military) clearances converted to industrial clearances.

In certain cases, however, the level of access that may be granted and the kinds of material that may be accessed - depends on restrictions that are imposed by the type of clearance itself. This is the case with interim clearances, contractor-granted clearances, and limited access authorizations.

## **INTERIM CLEARANCES**

Applicants submitted for SECRET and CONFIDENTIAL clearances are issued interim clearances, provided that the initial investigation fails to uncover any adverse information - that is, if checks of the records maintained in the Defense Clearance and Investigations Index (DCII), a review of the information on the EPSQ and the records that the contractor has on hand that pertain to the employee are favorable. By contrast, applicants submitted for TOP SECRET clearances are granted an interim TOP SECRET clearance only at the request of the head of the User Agency or designee with exceptions. Failure to obtain the approval will result in the individual being issued an interim SECRET clearance. Interim clearances are not valid for access to RESTRICTED DATA, FORMERLY RESTRICTED DATA, NATO, COMSEC, FOREIGN GOVERNMENT INFORMATION and SCI. The one exception to this rule is that an individual with an interim TOP SECRET clearance may access SECRET material with the above caveats.

## **CONTRACTOR - GRANTED CLEARANCES**

Under previous policy, contractors were delegated authority to act on behalf of the DoD to grant CONFIDENTIAL clearances to qualified employees. This authority was rescinded, though. Contractor - granted clearances in effect might remain valid until the 1 January 2004. These clearances are not valid for access to RESTRICTED DATA, FORMERLY RESTRICTED DATA, COMSEC, SCI, ACDA, NATO (except NATO Restricted) information, classified foreign government information, or for assignment to duty stations outside the U.S.

As a rule, only U.S. citizens are eligible for a security clearance and every effort should be made to ensure non-U.S. citizens are not placed into positions that may require access. However, there may be times within industry when an exception to the rule is called for. At such a time, a qualified immigrant alien or foreign national may be granted a Limited Access Authorization (LAA) at the SECRET or CONFIDENTIAL level.

A non-U.S. Citizen may be eligible for an LAA if the following criteria are met:

- The individual must possess a rare or unusual expertise.

- A qualified U.S. citizen cannot be hired in sufficient time to meet the contractual requirements.
- The appropriate Government Contracting Activity must concur.
- The Defense Security Service must concur.

You or your agency will become involved in this process since, prior to the facility submitting the LAA request to DISCO, they must obtain a written endorsement from the contracting officer having jurisdiction over the contract for which access is proposed. The LAA is terminated upon completion of the contract for which access was originally granted.

Note that LAAs granted under the NISP are not valid for access to TOP SECRET information, RESTRICTED DATA, FORMERLY RESTRICTED DATA, COMSEC, NATO, ACDA classified information, information for which a special access authorization is required, information determined not releasable to the individual's country, and information provided by a third party government.

## **INVESTIGATIVE POLICY: PROCEDURES**

The 13 eligibility criteria remain constant for all types and levels of clearance. What differs from type to type and level to level is the extent of investigative effort devoted to examining an individual's background. The higher the level of the clearance being sought, the greater the investigative effort or "scope." As a general rule, clearance below TOP SECRET entails electronic checks of various records, while a final TOP SECRET clearance entails both record checks and a series of interviews of the Subject and of those who have known the Subject.

DoD Directive 5200.2, "DoD Personnel Security Program" (issued to implement Executive Order 10450) prescribes the policy and general procedures, including the scope, which relates to the conduct of personnel security investigations. It was modified by National Security Directive 63 (NSD 63), issued by President Bush in October 1991. NSD 63 establishes the Single Scope Background Investigation, which replaces both the Background Investigation and the Special Background Investigation.

As amended by NSD 63, DoD 5200.2 stipulates that consideration for persons requiring access to classified information will be based upon one of two general types of investigations: 1. The National Agency Check (NAC) and 2. The Single Scope Background Investigation (SSBI). (DoD 5200.2-R, "Personnel Security Program Regulation," issued under the authority of DoD Directive 5200.2, contains expanded direction and procedures.)

## **NATIONAL AGENCY CHECK WITH LOCAL AGENCY CHECKS AND CREDIT CHECK (NACLCL)**

The most common type of investigation is the National Agency Check with Local Agency Checks and Credit Check (NACLCL), conducted when an applicant who is an U.S. citizen requires access to SECRET or CONFIDENTIAL information. The NACLCL is also the

investigative basis for an interim TOP SECRET clearance for certain individuals. The credit check portion of the NACLIC is the same as the credit check done for the Single Scope Background Investigation, described below.

## **AGENCIES QUERIED DURING THE NACLIC**

As a minimum, the following checks are conducted:

- First, investigators will conduct record checks at the appropriate courts for listed or developed criminal and/or public record information for the scope of the investigation. A electronic check for this activity may be conducted in lieu of the LAC if permitted by various electronic databases within the areas of scope of the investigation.
- Second, the Federal Bureau of Investigation (FBI) conducts search of two of their own file systems consisting of 1) name check of alphabetical indices maintained by the FBI Headquarters in Washington, D.C. to determine if an investigation was ever conducted on the individual; and, 2) a technical fingerprint search with the Identification Division to ascertain if the individual has ever been arrested or convicted of criminal activities. The technical fingerprint search requires that the applicant submit fingerprints for FBI analysis. These prints are then categorized and compared against fingerprints on file.

The third check made is with the Defense Clearance and Investigations Index (DCII). This is the central index of investigative files maintained throughout the DoD, including those records retained at the Personnel Investigations Center (PIC) within the DSS. A search of DCII may reveal the existence of the file number and location of reports of investigations which have previously been conducted (or are currently being conducted) by any DoD investigative agency, including the three military departments.

Other federal agencies may be checked as deemed appropriate to the case and the individual. For example, the Office of Personnel Management (OPM), formerly the Civil Service Commission, will be queried on persons who have been civilian employees of the United States Government, the United Nations, and other public international organizations. The Immigration and Naturalization Service (INS) will be queried if the applicant is a naturalized citizen or an immigrant alien, or if there are doubts involving the individual's citizenship. The State Department, particularly the Passport Division, maintains pertinent records of U.S. citizens who have applied for a passport. This department is generally checked when an individual whose parents are U.S. citizens was born outside the United States. The Central Intelligence Agency (CIA) may be contacted if there is a question involving the individual's foreign connections or foreign travel. If an individual was formerly in the Armed Forces, the master personnel records of the Military Personnel Records Center (MPRC) in St. Louis, Missouri, will be checked. Treasury Department files - such as those of the Secret Service, the Internal Revenue Service, and the Bureau of Customs - may also be reviewed if there is reason to believe they contain significant information. Finally, other federal agency files, such as those of the Coast Guard, may be checked when pertinent.

Further investigative efforts will be performed to substantiate or disprove unfavorable information or to resolve a matter disclosed during the conduct of a NACLIC.

## **SINGLE SCOPE BACKGROUND INVESTIGATION (SSBI)**

The second type of investigation is the Single Scope Background Investigation (SSBI). This type of investigation provides the basis for TOP SECRET access authorization and authorization for access to Sensitive Compartmented Information (SCI) or other information requiring special access approval. The SSBI also provides the basis for a SECRET LAA or a CONFIDENTIAL LAA. The SSBI makes inquiries into pertinent facts bearing on the suitability and trustworthiness of the individual taking into account both positive and negative factors. The SSBI is designed to develop information upon which to base decisions regarding access authorizations, so that those granted will be clearly consistent with the national interest.

Procedures for conducting the SSBI are considerably more complicated and time-consuming than those of the NAC. The period of investigation for an SSBI covers the last ten years of a Subject's life, or from the 18th birthday, whichever is shorter. The SSBI always includes a NAC of the Subject, as described above.

### **COMPONENTS OF THE SSBI**

In addition, a NAC of the Subject's spouse or cohabitant and any non-U.S. citizen family members are conducted.

An interview of the Subject is conducted at the beginning of the investigation in order to determine essential information about the individual. This interview is normally conducted at the Subject's place of employment and normally lasts from one to two hours.

Interviews of former spouses are also conducted if the divorce occurred during the period of investigation.

When the applicant claims U.S. birth and citizenship, these are verified by the requester of the clearance, and an independent verification is made by DSS.

Credit bureau checks are conducted in the areas where the subject has worked, resided, or attended school for 6 months or more during the period under investigation.

Local Agency Checks (LACs), such as checks of files of the state police in areas where the subject has resided for a total of 6 months or more during the period of investigation, are also conducted.

A neighborhood investigation verifies the Subject's current residence, and two neighbor references are interviewed in each area where the Subject lived for a total of 6 months or more during the past 5 years.

Education records are also checked which reflect the Subject's most recent or most significant education within the period under investigation.

Public records that reflect the Subject's divorce(s), bankruptcy, and similar matters are checked.

All employment records within the period under investigation are checked. This check also includes employment references, interviews preferably with the Subject's supervisor and a co-worker. Exceptions to the interview portion of the check are for part-time and seasonal or temporary jobs (jobs of four duration or less).

Also, unemployment of more than 60 days during the period of investigation is checked.

Four character references whose combined association with the Subject covers the entire period under investigation will be interviewed. Three of the four must be "developed character references," that is, persons not listed on the Personnel Security Questionnaire.

An SSBI may include other checks, such as a check of Subject's medical records (especially those which reflect a history of mental or nervous disorders).

## **PERIODIC REINVESTIGATION**

Granting an initial clearance is not the end of the security clearance process. Continuing evaluation of the individual's suitability to hold the clearance is essential. One formal aspect of this continuing evaluation is the Periodic Reinvestigation (PR).

The PR is conducted at 5 year intervals after the initial clearance is granted. An extensive PR is conducted on cleared individuals having access to TOP SECRET, Sensitive Compartmented Information, and other selected special access programs, while a less extensive PR (NACLC and Credit Bureau Checks only) is conducted on other cleared individuals.

## **CHART**

The chart on the next page summarizes the investigative requirements and the investigative scoping that we have been discussing.

**CLEARANCE OF INDUSTRIAL PERSONNEL  
INVESTIGATIVE REQUIREMENTS**

U.S. CITIZENS			IMMIGRANT ALIENS & FOREIGN NATIONALS	
	TOP SECRET (SCI) or other special access	TOP SECRET	SECRET/ CONFIDENTIAL	SECRET LAA/CONFIDENTIAL LAA
Final	SSBI	SSBI	NACC	SSBI
Interim	Not Authorized	NACC	DCII and Available Records	Not Authorized

**INVESTIGATIVE SCOPE**

NATIONAL AGENCY CHECK With Agency Checks AND CREDIT CHECK (NACLC)	
Defense Clearance and Investigations Index (DCII)	Federal Bureau of Investigation (FBI)
Subject's name is checked against names that appear in documents of DoD agencies that investigate criminal, counterintelligence, fraud, and personnel security matters.	<ul style="list-style-type: none"> <li><b>FB11H0.</b> Subject's name is checked against names in FBI's investigative files.</li> <li><b>FBIVID.</b> Subjects fingerprints are checked against FBI's file of fingerprints submitted by law enforcement agencies.</li> </ul>
<ul style="list-style-type: none"> <li><b>Local Agency Checks</b></li> <li><b>Credit Bureau Check</b> as described under SSBI below.</li> </ul>	

**and**

Agency	If Subject:	Agency	If Subject:
Office of Personnel Management (OPM)	<ul style="list-style-type: none"> <li>- was U.S. Gov't civilian employee</li> <li>- was U.S. citizen employee of U.N.</li> <li>- had NRC or DOE clearance</li> </ul>	Central Intelligence Agency (CIA)	<ul style="list-style-type: none"> <li>- resided outside U.S. for a year or more since age 18</li> <li>- was a CIA employee</li> <li>- resided, traveled, was educated or employed since age 18 in a Designated country</li> </ul>
Immigration and Naturalization Service (INS)	<ul style="list-style-type: none"> <li>- is an alien in the U.S.</li> <li>- is a naturalized U.S. citizen (unverified)</li> <li>- is an immigrant alien</li> <li>- is a U.S. citizen through parent's naturalization (unverified)</li> </ul>	Military Personnel Record Center (MPRC)	- served in U.S. Armed Forces during the last 15 years
State, Department - Security Division (S/D) - Passport Division (P/D)	<ul style="list-style-type: none"> <li>- was a State Dept employee</li> <li>- is a U.S. citizen through birth abroad to U.S. parents (unverified)</li> </ul>	Treasury Department (Secret Service, Internal Revenue Service, Bureau of Customs)	[Only if available information indicates that a TD agency has pertinent information]
		Other agencies (e.g., Coast Guard)	[Only when pertinent to purpose of investigation]

SINGLE SCOPE BACKGROUND INVESTIGATION (SSBI)	PERIODIC REINVESTIGATION (PR)*
PERIOD OF INVESTIGATION (POI) Past 10 years or to age 18, whichever is less	Past 5 years

**NATIONAL AGENCY CHECK (NAC) of Subject**

NAC of spouse or cohabitant and any family members not U.S. citizens	Any current spouse, cohabitant, or alien family NAC not previously done for SSBI
----------------------------------------------------------------------	----------------------------------------------------------------------------------

**INTERVIEW OF SUBJECT**

INTERVIEWS OF FORMER SPOUSES whose last date of marriage of Subject is within the POI
DATE AND PLACE OF BIRTH (DPOB) verified. (Subject provides birth certificate)

**CITIZENSHIP**

Verify U.S. citizenship if Subject claims. For Subjects who are not U.S. citizens and for all foreign-born immediate family members, verify citizenship or legal status in U.S.

**CREDIT BUREAU CHECKS**

Wherever Subject lived, worked, or attended school for 6 months or more during the POI or the past 7 years, whichever is shorter

**LOCAL AGENCY CHECKS**

Where Subject lives and wherever Subject lived, worked, or attended school for a total of 6 months or more during the POI

**NEIGHBORHOOD INVESTIGATION**

Verify current residence. 2 neighbor references in each area where Subject lived for a total of 6 months or more during the past 5 years	SSBI requirement, if not previously met
------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------

**EDUCATION RECORDS**

Most recent or most significant attendance/degree diploma within POI. If no education within POI, last education above high school level.	SSBI requirement, if not previously met
-------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------

**PUBLIC RECORDS** of divorce(s), bankruptcy, etc., and any other court actions

**EMPLOYMENT RECORDS**

At all places of employment within POI or past 2 years, whichever longer. Federal employment/military service records are verified requester.	At current employment and wherever employment references are interviewed
-----------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------

**EMPLOYMENT REFERENCES - Interviews with supervisors/co-workers**

2 references at each employment of 6 months or more within the POI and each period of military service of 6 months or more within the past 5 years	2 references at most recent employment of 6 months or more
----------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------

**UNEMPLOYMENT of more than 60 days within the POI**

**CHARACTER REFERENCES**

4 references whose combined association with Subject covers the POI; 3 must be developed, but 1 may be listed by Subject	2 developed references whose combined association with Subject covers the POI
--------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------

\* The PR for a SECRET clearance is also conducted at 5-year intervals but consists of a NAC and CREDIT BUREAU CHECKS only.

## **LIMITED INQUIRY AND POST - ADJUDICATIVE INVESTIGATION**

Two other investigations are occasionally conducted on industrial personnel: the Limited Inquiry and the Post-Adjudicative Investigation. These investigations are conducted to resolve information surfaced during an ongoing investigation (the limited inquiry) or subsequent to a previous investigation (the post-adjudicative investigation). The scope of each is limited to the type and amount of investigation necessary to resolve the issue.

## **CONTRACTOR'S RESPONSIBILITIES: INITIAL PROCESSING**

In complying with the NISP, a contractor must fulfill certain responsibilities when processing an employee for a personnel security clearance. First of all, the contractor must determine that the clearance is needed in order for the employee to perform tasks or services essential to the fulfillment of a contract or program requiring access to classified material. In other words, the contractor recognizes the applicant's need for access to classified information in order to successfully accomplish the assigned duties. In all cases, it is the responsibility of the contractor to limit the number of personnel processed for clearances to the extent possible consistent with contractual obligations. For instance, the contractor must ensure that clearances are not used as a status symbol within the facility.

Secondly, the applicant must be on the payroll of the contractor before being processed for a clearance. Being "on the payroll" means the employee will receive some type of remuneration for services. The exception to this prerequisite is:

Where a written agreement between the contractor and prospective employee for future employment exists, which stipulates a fixed date for entry on the payroll (normally within 30 days), as in the case of a college student who will report to work after graduation. In this instance, prior to the applicant's entry on the payroll, the contractor may submit an application for a clearance, provided the agreement stipulates the actual (fixed) date of entry on duty is not contingent upon the issuance of a personnel security clearance.

Once the employee has been advised of the requirement to be processed for a security clearance by the contractor, the individual is briefed on the Privacy Act of 1974, which identifies the necessity for providing the information requested on the personnel security questionnaire - the SF 86. In effect, the contractor is acting as an agent for the federal government and should ensure that the applicant understands his or her rights as stated in the Privacy Act of 1974. DSS uses an electronic version of the SF 86 known as the EPSQ. (EPSQ software can be downloaded at [www.dss.mil](http://www.dss.mil). A screen at the beginning of the form explains the privacy act provisions.)

## **DEFENSE INDUSTRIAL SECURITY CLEARANCE OFFICE**

When a contractor is satisfied that all initial requirements for clearance processing have been fulfilled, the request for clearance and the appropriate forms are completed and sent to the Defense Industrial Security Clearance Office (DISCO) in Columbus, Ohio. DISCO, which is under the direction of the Deputy Director for Security Programs for DSS, receives

and processes over 20,000 requests for clearances from industry every month. Specifically, DISCO performs the following functions:

- Screens requests for clearances and initiates paperwork for the necessary investigations
- Processes requests for interim clearances
- Issues a Letter of Consent when a clearance is granted
- Processes reinstatements and conversions of prior clearances
- Furnishes foreign governments and contractors with security assurances on U.S. personnel and facilities
- Maintains a central facility address file
- Maintains and updates pending and closed case files on contractor personnel
- Maintains the current status of a contractor employee's clearance
- Provides worldwide distribution for DoD and DISCO forms pertaining to the NISP

## **PERSONNEL INVESTIGATIONS CENTER**

For an initial clearance, DISCO checks to see that the personnel clearance applications submitted by the contractor are complete and accurate and forwards them to the Personnel Investigations Center (PIC) at Fort Meade, Maryland.

Like DISCO, the PIC is part of DSS. PIC, however, services all of DoD, that is, it receives all DoD security applications from a variety of requesters, including DISCO. If you are cleared or have been cleared in the past, your clearance request was most likely processed at the PIC.

As you know, when a TOP SECRET clearance is requested an SSBI is required as the investigative basis for it. To accomplish the SSBI, PIC sends out the security application, with the investigative leads (record checks and interviews) to be conducted, to those DSS field offices responsible for the areas where the applicant has lived, worked, or attended school during the period of investigation. Each field office completes its leads and sends a report of investigation (ROI to PIC). Through its screening program; PIC reviews the investigative findings to determine the applicant's suitability for a security clearance.

If DISCO can make a clear determination that the TOP SECRET clearance should be granted, i.e., if there is no significant derogatory information, the report of investigation is returned to DISCO. DISCO then transmits a Letter of Consent (LOC) to the applicant's facility stating that the individual may be permitted access to classified information up to the TOP SECRET (or TOP SECRET -SCI) level. These have been sent over the internet since February 2002.

PIC, like DISCO, does not deny clearances. When DISCO and PIC are unable to make a clear determination that a clearance should be granted based on the information reviewed in the applicant's Personnel Security Questionnaire, the ROI, and other documents (in other words, when a case contains major derogatory information), DISCO refers the case to the Defense Office of Hearings and Appeals (DOHA) for review to grant or deny the clearance.

## **CLEARANCE DENIAL AND REVOCATION**

From the founding of the program until 1959, there were a number of court cases dealing with industrial security. For the most part, these cases were brought by employees of defense contractors who had been denied clearance by one of the Industrial Security Boards established by the Department of Defense for the purpose of adjudicating industrial security cases. Essentially, the decisions reached prior to 1959 upheld the DoD and sanctioned the decisions that resulted in the denial or revocation of personnel security clearances. The case of *Greene v. McElroy*, unlike the others, reached the Supreme Court and resulted in a different decision.

### **EXECUTIVE ORDER 10865**

As a result of the Supreme Court's decision in favor of *Greene*, Executive Order 10865, "Safeguarding Classified Information Within Industry," was issued in February, 1960. The purpose of the executive order was two-fold: first, to help ensure against the unauthorized disclosure of classified information entrusted to U.S. industry, and second, to protect the constitutional rights of the industrial applicant for a personnel security clearance. E.O. 10865 provided the authoritative basis for industrial security clearances that the Supreme Court in its ruling had found lacking, and it specifically guaranteed an applicant whose clearance was denied the opportunity to cross-examine accusers.

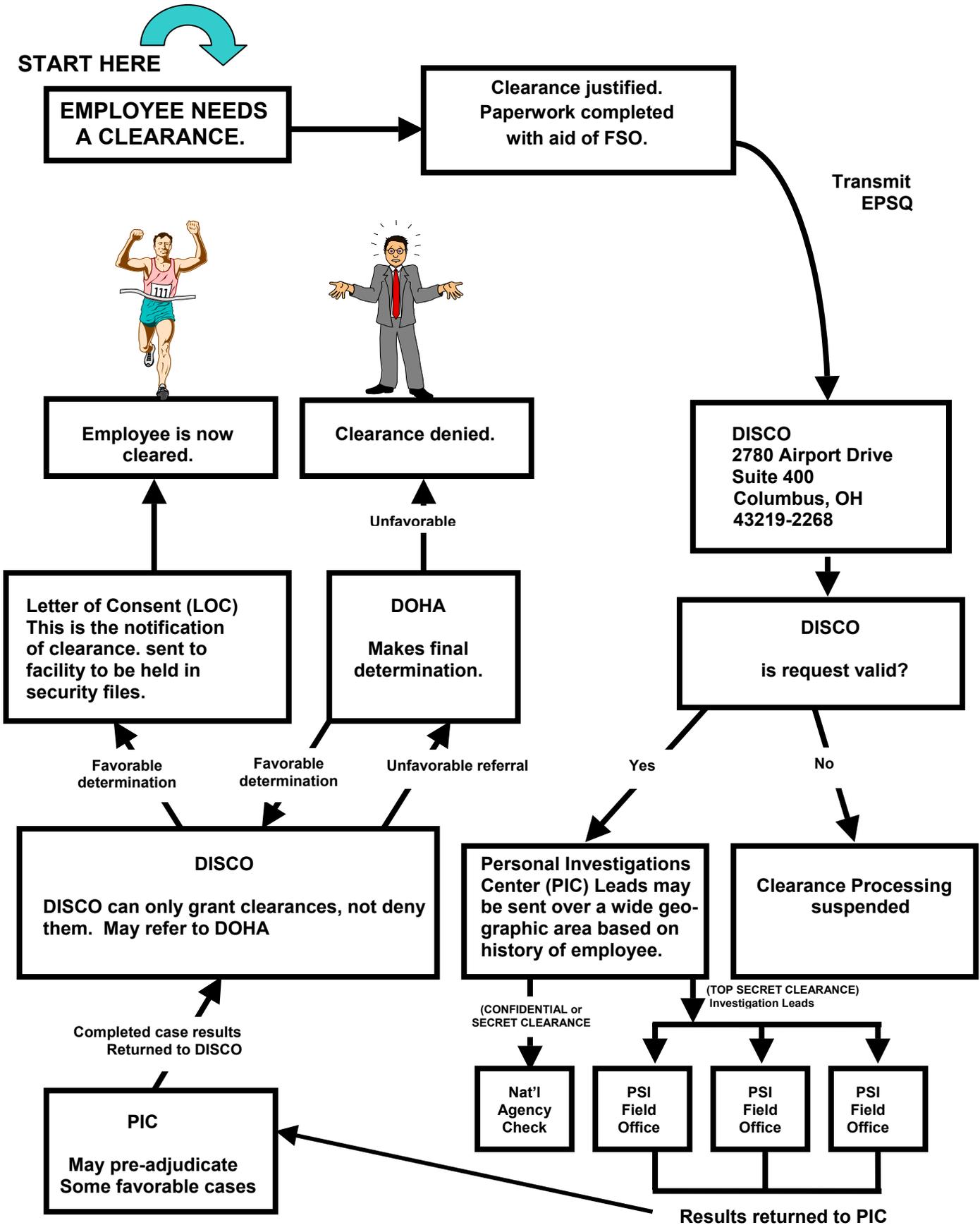
These provisions of E.O. 10865 were implemented through DoD Directive 5220.6, "Defense Industrial Personnel Clearance Review Program," which is the basis for the operating procedures of the Defense Office of Hearings and Appeals (DOHA). We'll be examining these procedures in detail in a moment, but first let's look at the provisions themselves.

Under E.O. 10865 an industrial personnel security clearance cannot be denied or revoked unless the individual is given:

1. A written statement of reasons why the clearance is denied or revoked
2. A reasonable opportunity to reply to the statement of reasons
3. A chance to make a personal appearance before a government authority
4. A reasonable time to prepare a case
5. An opportunity to be represented by legal counsel
6. An opportunity to cross-examine accusers
7. Upon conclusion of all proceedings, written notice of the government's final decision

E.O. 10865, therefore, provided the mandate and the impetus for revamping the government's procedures for clearing industrial personnel. It led directly to the establishment of the organization that is authorized to deny and revoke industrial personnel security clearances.

# LIFE CYCLE OF A PERSONNEL SECURITY INVESTIGATION



## **DEFENSE OFFICE OF HEARINGS AND APPEALS (DOHA)**

The chief function of the Defense Office of Hearings and Appeals (DOHA) is to review investigative reports and recommendations from PIC and, when warranted, to deny, suspend, or revoke clearances. DOHA has the authority to request additional investigations at any point during its review process. In an emergency, the Director of DSS has the authority to suspend a clearance for a period of one year. DOHA may suspend a clearance indefinitely.

DOHA's headquarters is in Arlington, Virginia. Although Personnel Security Divisions II & III of DOHA are collocated with DISCO in Columbus, Ohio, DOHA is not a part of DSS. DOHA reports to the Office of the General Counsel, Office of the Secretary of Defense.

### **REVIEW PROCEDURES**

When DISCO sends a clearance request to DOHA for determination, the following procedures are set in motion:

#### **1. Adjudication by Personnel Security Division.**

The case is examined by an adjudicator in the Personnel Security Division, who reviews the investigative file and determines whether access should be granted or denied. If the adjudicator decides the clearance should be granted, the case is returned to DISCO, which then sends out the Letter of Consent (LOC) to the applicant's facility.

If the decision is to not grant the clearance, the adjudicator will draft a statement of reasons (SOR) for the denial. The case, along with the SOR, is sent to the Personnel Security Division in Arlington, Virginia.

Following a review of the paperwork by a general counsel for legal sufficiency, the SOR is sent to the applicant explaining the reason for the clearance denial. The applicant then has 20 days to reply. If no reply is made, DOHA will discontinue processing the clearance application or take action to revoke the existing clearance. In the case of a revocation, the adjudicator may recommend a suspension of a clearance for up to one year, pending further proceedings.

#### **2. Review by Hearing Examiner.**

Should the applicant reply to the SOR and request a hearing, the case is referred to a hearing examiner, a qualified attorney assigned to DOHA by the Office of General Counsel, who reviews the case and the applicant's reply. A hearing is held. The purpose of the hearing is to obtain additional facts in the case in order to reach a fair and impartial determination. This is the applicant's only opportunity for full cross-examination and confrontation of accusers within the DOHA review process. Although the hearing procedures are formal in nature, the technical rules of evidence are relaxed to permit all relevant information to be addressed during the course of the proceedings. The examiner then has 30 days to prepare a final recommendation. The applicant is informed of the examiner's decision and the applicant (if denial is recommended) or the

government (if granting the clearance is recommended) may appeal the decision. If an appeal is to be made, a written notice of intent to appeal must be filed within 20 days. The actual appeal must be filed within 60 days.

### **3. Decision by Appeal Board.**

The written appeal to the hearing examiner's decision then goes before the three-member Appeal Board, appointed by the Office of the General Counsel, which makes a decision based upon majority rule. The Appeal Board then prepares a written statement of its final decision. At this point, further recourse for the applicant is available through the civil court system.

### **4. Reconsideration by DOHA.**

An individual may have his/her eligibility for a clearance reconsidered at any time by DOHA upon showing newly discovered evidence or other good cause. Normally DOHA does not reconsider clearance eligibility for at least one year.

## **CONTRACTORS RESPONSIBILITIES AFTER CLEARANCE GRANTED**

Once an individual is cleared, we rely on the contractor to assist us in an ongoing assurance that the individual's clearance should be continued. Unfortunately, many people have the mistaken notion that personnel security is simply the conducting of an investigation and the issuance of a clearance. Nothing could be further from the truth. As we have noted, the issuance of a clearance marks the beginning of the process of continuing evaluation that includes the PR.

An important aid in ensuring that the continuing evaluation of the cleared employee remains favorable is the contractor's security education and training, designed to provide the cleared individual with the proper motivation and knowledge necessary to carry out security responsibilities.

Another critical ingredient is the contractor's responsibility to monitor the individual's behavior from a security standpoint and to report in accordance with I-302a, NISPOM, to DISCO whenever information develops that may suggest the individual's continued access to classified information may not be clearly consistent with the national interest. We call such information adverse information. A cleared employee's excessive use of alcohol, illegal use of drugs or controlled substances, psychiatric problems, arrests, and similar changes in behavior are examples of some of the items that should be reported. As a general rule, the 13 clearance eligibility criteria that were applied originally in determining the individual's suitability for a position of trust continue to be the criteria by which an employee's suitability for his or her clearance is assessed.

Contractors should not hesitate to make adverse information reports on individuals who exhibit or are reported as involved in one or more of the 13 conditions. And yet, even though such involvement may be grounds for the suspension or revocation of a security clearance by the government, the involvement is sometimes overlooked or not reported, perhaps from an unwarranted concern that the individual involved will seek legal redress. In fact, contractors are not liable for defamation of an employee because of reports made

to the government. The cases of Becker v. Philco and Taglia v. Philco (389 U.S. 979) addressed this point and established strong case law for contractor immunity from liability.

## **SUMMARY**

The contractor environment differs from the military or government civilian environment with which you are familiar. Because of this, the forms and procedures involved in granting, denying, suspending or revoking an industrial personnel clearance are different. In certain cases, the GCA plays a role in the requesting of clearances. Interim TOP SECRET clearances and limited access authorizations require approval of the GCA. The contractor is also obligated to file certain reports for all cleared personnel.

## REVIEW EXERCISES

Complete the following exercises for review and practice.

1. Eligible non-U.S. Citizens may be granted a L\_\_\_\_\_ A\_\_\_\_\_  
A\_\_\_\_\_.
2. A National Agency Check with LAC and Credit Check is the investigative requirement for a S\_\_\_\_\_ or C\_\_\_\_\_ clearance.
3. The D\_\_\_\_\_ C\_\_\_\_\_ and I\_\_\_\_\_ I\_\_\_\_\_ is the central index of investigative files maintained by the Department of Defense.
4. As part of an SSBI, U.S. birth and citizenship are always verified by an U.S. Government agency, usually DSS for industrial cases.  
  
True  
False
5. The D\_\_\_\_\_ I\_\_\_\_\_ S\_\_\_\_\_ Clearance Office issues the Letter of Consent when a clearance is granted.
6. The P\_\_\_\_\_ Investigations Center receives the clearance request and sends the investigative leads to be conducted to the various DSS Field Offices.
7. The case of \_\_\_\_\_ v. \_\_\_\_\_ addressed the right of an applicant for an industrial security clearance to confront and cross-examine accusers.
8. If the determination has been made to deny the clearance by the Defense Office of Hearing and Appeals the S \_\_\_\_\_ of R \_\_\_\_\_ is sent to the applicant, who must respond within \_\_\_\_\_ days.

## **ANSWERS**

1. *Limited Access Authorization (p. 2-4)*
2. *SECRET, CONFIDENTIAL (pp. 2-5)*
3. *Defense Clearance and Investigations Index (pp. 2-6)*
4. *True (pp. 2-7)*
5. *Defense Industrial Security (p. 2-11)*
6. *Personnel (p. 2-11)*
7. *Greene, McElroy (p. 2-12)*
8. *Statement of Reasons  
20 (pp. 2-14)*

## LESSON 3

# Visitor Control

Visitor control procedures are essential in order to prevent visitors from gaining unauthorized access to classified information. Section III of the Industrial Security Regulation (DoD 5220.22-R) establishes the procedures and responsibilities of the User Agency for classified visits. Procedures for the contractor are contained in the National Industrial Security Program Operating Manual (NISPOM), DoD 5220.22-M, Chapter 6.

## OBJECTIVES

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

- Discuss the general requirements for a classified visit.
- List the information required on a Visit Authorization Letter (VAL).

## BASIC CONCEPTS

Because you and your personnel visit contractors and vice versa, you need to know the procedures that the contractors are expected to follow under the NISP. You will find that some of the requirements are not what you're used to following.

Who is considered a "visitor"? Within the NISP, a visitor may be defined as "any non-employee requiring access to classified information at your location." If the visit can be accomplished without having access, they are not considered a visitor under the NISP.

Some of the basic concepts regarding visits are:

- Keep the visits to an absolute minimum required to effectively meet contractual requirements.
- Be sure there is a need-to-know (not nice to know!).
- Be sure the individual has the authority to gain access.
- If you disapprove of the visit, notify the sender. If you don't, the sender is to assume that the visit has been approved.

## VISIT AUTHORIZATION LETTER

The following items of information must appear on the VAL:

- Name of individual to be visited. This can be used to verify the need-to-know.
- Name, POB, DOB, and citizenship of the visitor.
- Clearance Level: To include any restrictions or special access approvals.
- Purpose of the Visit: This is an important part of the VAL. This should contain as much information as necessary to allow the receiver to make a determination on whether or not to grant the visit.

- Period or Duration: Classified visits may be arranged for a 12-month period or another period that is appropriate for the purpose of the visit. If the visits are contract related, the VAL could cover the life of the contract. You may accept the VAL for whatever period you deem appropriate within these parameters.
- Necessary Information: Name and address of sender, to include Commercial and Government Entity (CAGE) code and phone number. This could be on official letterhead. Obviously, User Agencies do not have CAGE codes. (CAGE codes are issued to companies doing business with the federal government.)
- Level of Facility Clearance: The contractor must provide you this information. You in turn should contact the Defense Security Service, DISCO, Central Verification Activity (CVA) in Columbus, OH and verify this information unless the two parties have a current contractual relationship at the same or higher classification level. The most efficient way to contact CVA is via the internet at [www.dss.mil](http://www.dss.mil). The Regulation states that once you have verified the fact that the facility is in the program, if you have any doubt regarding the visitor's clearance you will contact the security officer of the facility that sent the VAL. You should not call DISCO and attempt to verify the clearance through them.

As you can see, the visitor's Social Security Number (SSN) is not required. The Privacy Act of 1974 requires a Federal activity to provide an individual with a Privacy Act statement when requesting the individual's SSN. Most contractors know, however, that the User Agencies and other contractors sometimes do not accept VALs unless the SSN is included.

## **VISITING CONTRACTOR'S RESPONSIBILITIES**

How do these VALs get from one place to the other? The VAL must be made in writing and in advance of the visit. It cannot be hand carried by the visitor (it may be transmitted by a courier). Should a contractor show up at your installation hand carrying his or her own VAL you shouldn't authorize access until you receive a VAL from the facility directly. The facility is allowed to telephone the VAL information to you as long as they follow up with a hard copy. The decision to accept the phone information is left up to you.

This applies to your visit to them also. Travel orders are not considered a valid VAL under the NISP. Acceptable methods of sending a VAL include a letter, facsimile transmission (Fax), and teletype. Electronic means, such as e-mail, are also acceptable, when access to the program is controlled through physical or software protection and has digital signature authentication.

It is the sender's responsibility to notify the receiver of any changes to the information provided in the VAL.

## **ACTION BY THE RECEIVER**

The receiver, using the information on the VAL, may approve or disapprove the visit. Note that the receiver of the VAL must notify the sender only when the VAL is disapproved. The appropriate clearance level and need-to-know must be considered. Can the visit be conducted without the individual receiving access to classified information? If so, then approve an unclassified visit and send the VAL back.

It was mentioned that the facility clearance must be verified. Contacting CVA was one method. The other would be if you already have a contractual relationship with the facility and the contract is at that particular clearance level or higher. Thus, the facility clearance should have been verified previously. These verifications are valid for a period of three years or as long as the contract remains valid. During that period you will be notified by CVA of any changes in the information previously provided to you.

When the visitor arrives, make sure you verify the fact they are who they say they are by viewing something with their name and picture on it, such as a driver's license or employee ID card. Keep a record of all visitors approved for access to classified information. The record must indicate the visitor's name, the name of the activity represented, and the date of the visit.

Many contractors will not allow visitors to carry in cameras, cell phones, personal digital assistance (PDAs) devices, video equipment, tape recorders, and the like, so be sure to brief your personnel regarding the rules prior to their visit to a contractor. Be aware that approval for the visit only authorizes access to classified information, not physical release of classified material. Release would be authorized only if done through proper procedures or channels. One of the biggest offenders of this is the "good old boy" network. Release of classified material should be limited to only those facilities who have a bonafide need, are authorized access to it, and have proper storage capability.

## **CATEGORIES OF VISITORS TO CONTRACTORS**

The NISPOM discusses two categories of visitors. The two categories are as follows:

**Contract Related Visits** are those in which there is a contractual relationship (to include all phases of pre-contract activity) between the sender and the receiver. In this case the VAL goes directly from the sender to the receiver.

**Non-Contract Related Visits** are those in which there is a need-to-know and the appropriate clearance level, but no contractual relationship exists. When this situation exists, the party who will be disclosing the classified information must seek approval from the Government Contracting Activity (GCA) jurisdiction over the information. User Agencies can, however, process their VALs directly, provided that it is their classified information, which will be accessed. If the classified information belongs to another User Agency (UA) (or to a Non-User Agency), the VAL may have to be processed through that agency for a release authorization.

## **VISITS BY DEPARTMENT OF ENERGY (DOE) PERSONNEL TO DoD FACILITIES**

When representatives of DOE and its contractors visit a DoD UA contractor's facility for the purpose of having access to a DoD UA's classified information, the visit is a Non-Contract Related Visit. As such, it requires a need-to-know certification by the DoD UA that has jurisdiction over the information involved.

The DOE activity requesting the visit will furnish the required information to the DoD UA whose information is involved using DOE's form, "Request for Visit or Access Approval," DOE Form 5631.20.

If approved, the DoD UA will forward the DOE Form 5631.20 to the contractor with the certification of the need-to-know for the visit.

Contractors may accept the clearance information contained in the DOE Form 5631.20 provided it contains a DoD UA's endorsement and the visitor presents proper identification at the time of the visit.

## **VISITS TO DOE ACTIVITIES AND DOE CONTRACTORS**

Contractor visits to DOE activities and DOE contractors are also considered Non-Contract Related visits and are forwarded to the DOE through the appropriate DoD UA for need-to-know certification and personnel clearance certification. These requests do not have to be made on the DOE form as long as the request contains all the required information. However, DoD activities must follow DoD Directive 5210.2.

## **VISITS INVOLVING OTHER NON-USER AGENCIES**

Visits to or by other Non-UA's are also considered Non-Contract Related visits. Visit requests are forwarded through the appropriate GCA for disclosure certification if access to UA classified information is involved.

## **VISITS TO USER AGENCY ACTIVITIES OUTSIDE THE UNITED STATES**

Visits to UA activities outside the U.S. are processed in the same manner as other classified visits. The overseas activity to be visited will notify the contractor of the approval or disapproval of the visit request.

## **CLASSIFIED MEETINGS**

The general policy is that all meetings within the scope of the Industrial Security Regulation (ISR) (paragraph 1-400) must be sponsored by a DoD component. Exceptions to this rule include the following:

- Meetings related to a specific contract or project, including pre-proposal or pre-award meetings
- Post-award briefings conducted by the DoD contracting activity
- Meetings conducted by a cleared contractor(s) and attended by cleared contractor personnel directly involved in the performance of a contract or project
- The head of the component having a significant interest in the subject matter may sponsor a meeting after determining that the meeting is in the best interest of the national security
- The use of conventional channels for dissemination of classified scientific and technical information would not accomplish the purpose of the meeting
- Adequate security measures and access procedures have been developed and will be carried out
- The location selected for the classified sessions of the meeting facilitates the proper control and dissemination of classified information and adequate facilities are available for its storage and protection.

## **REQUESTS FOR SPONSORSHIP**

Contractors desiring to conduct meetings requiring sponsorship will submit their requests to the UA having principal interest in the subject matter of the meeting. Only that UA may sponsor the meeting. Details regarding necessary information and other security precautions are addressed in paragraphs 6-201 through 6-203, NISPOM, as well as in 1-400 through 1-410, ISR.

## **SUMMARY**

There are certain basic requirements set forth for the control of visitors as well as responsibilities of the requesting contractor and the User Agency activities. Remember as you accept visitors and the contractor approves visit requests you are both authorizing disclosure of your classified information. It is vital to the protection of classified information that the visitor fully understands the requirements set forth, and the rationale behind these requirements, in the NISPOM and ISR. Requirements levied on the contractor in addition to those in the NISPOM are at the discretion of the User Agency; however, the User Agency may have to bear the costs, depending on the circumstances.

## REVIEW EXERCISES

Complete the following exercises for review and practice. Multiple choice questions may have one or more correct choices.

1. A visitor is any non-employee who requires a \_\_\_\_\_ to c\_\_\_\_\_ information.
2. A VAL must contain which of the following?
  - a. Name of visitor
  - b. Visitor's date & place of birth
  - c. Visitor's Social Security Number
  - d. Visitor's clearance level
  - e. Date & issuing authority of visitor's clearance
  - f. Facility clearance level & CAGE code of the sender
3. A VAL sent by facsimile (fax) is acceptable.  
  
True  
False
4. Official government travel orders may serve as a VAL to a contractor's facility.  
  
True  
False
5. A visitor's identification must include the visitor's n\_\_\_\_\_ and p\_\_\_\_\_.
6. A facility clearance must be verified and this can be done by contacting the DSS, D\_\_\_\_\_, - C\_\_\_\_\_.
7. There are \_\_\_\_\_ visit categories.
8. Visits to User Agency activities outside the United States must be forwarded through DISCO.  
  
True  
False
9. A User Agency must formally sponsor a classified meeting at a cleared facility.  
  
True  
False
10. Meetings may be sponsored by a DoD component only when the head of the component determines that the meeting \_\_\_\_\_.

## **ANSWERS**

1. *access to classified information (p. 3-1)*
2. *a; b; d; f; (pp. 3-1,2)*
3. *True (p. 3-2)*
4. *False (p. 3-4)*
5. *name picture (p. 3-3)*
6. *DISCO, CVA (p. 3-2)*
7. *two (p. 3-3)*
8. *False (p. 3-4)*
9. *True (p. 3-5)*
10. *is in the best interest of the national security (p. 3-5)*

## LESSON 4

# Classification Management

"Classification Management" (CM) is the system within the DoD for identifying that official information which requires protection in the national interest (classifying); how much protection (level of classification), and for what period of time protection is required (duration). It's basically the system our government employs to exercise control and management over its national security information. Within the NISP, industrial facilities are provided, generate, and handle national security information (classified material). Defense contractors are required to effectively safeguard and manage (protect) the classified material to which they have access.

In order to protect the material it handles or generates, contractors must know what is classified, at what level, and for how long. Under the terms of the Security Agreement (DD Form 441), the government is obligated to provide contractors with classification guidance. This is accomplished by indicating "by security classification (TOP SECRET, SECRET, or CONFIDENTIAL) the degree of importance to the national security of information pertaining to supplies, services, and other matters to be furnished by the Contractor to the Government or by the Government to the Contractor." Further, "the Government shall give written notice of such security classification to the Contractor and of any subsequent changes thereof."

CM within the NISP includes the receipt, application, and utilization of proper classification guidance and instructions; the assignment of appropriate derivative classifications, declassification, and other required markings; and, the regrading of classified materials.

## OBJECTIVES

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

- Recognize and explain the components of CM and discuss their importance to the NISP.
- Describe the general policies and procedures of Executive Order 12958.
- Distinguish between original and derivative classification, and explain the basic principles of derivative classification.
- Identify the requirements for issuance, purpose, and uses of security classification guidance (DD Form 254 and classification guides).

## CLASSIFICATION PROCESS

Why do we have a classification process and what do we mean when we talk about a classification process? History has shown that almost every administration has executed an executive order pertaining to the NISP. Executive Order (E.O.) 12958, issued by President Clinton, establishes policy and procedures for the government's Information

Security Program and CM in the NISP. The Information Security Oversight Office (ISOO) is the government activity designated in E.O. 12958 to be responsible for monitoring the information security programs of all executive branch agencies that create or handle national security information. Originally established under Executive Order 12065, ISOO remains the primary organization charged with the oversight prescribed by President Clinton's E.O. of April 17, 1995. Although ISOO is an administrative component of the National Archives Records Administration (NARA), it receives its policy guidance from the National Security Council. ISOO has developed a slide-tape presentation, which discusses the classification process and its history. It would be beneficial for you to obtain a copy from ISOO to include in your security education briefings. A copy can be obtained from the Director, ISOO, National Archives and Records Administration, Seventh and Pennsylvania Avenue, N.W., Washington, D.C. 20408.

Let's take a brief look at the Information Security Program. As we mentioned, E.O. 12958 establishes policy and procedures for the government's Information Security Program (ISP) and for CM in the NISP. It provides instructions on how to properly mark and safeguard classified information.

Implementation of E.O. 12958 is by means of ISOO Directive Number 1. All of our directives and regulations are driven by this ISOO Directive. In turn, DoD Directive 5200.1, the DoD Information Security Program, provides for the authority to issue DoD 5200.1-R, the Information Security Program Regulation. This regulation applies to OSD, Military Departments, Unified & Specified Commands, and the various Defense Agencies. The National Industrial Security Operating Manual (NISPOM) was developed to serve the needs of the departments of defense and energy, the Nuclear Regulatory Commission, and the Central Intelligence Agency. The NISPOM is provided to each cleared contractor facility and is, in fact, a part of the Security Agreement (DD Form 441).

## **CLASSIFYING INFORMATION**

As you know, information can be classified in one of two ways: originally or derivatively. Information which meets certain criteria may be classified originally by designated government officials. The derivative process is accomplished by government or contractor personnel who derive the classification to be assigned to new material from something already classified by an original classifier. In this process the level of classification is determined based on the degree of damage to the national security should the information be compromised. Also, the duration of the classification is determined. A specific date or event for declassifying the information must be determined.

Since no contractor has original classification authority, how does a contractor classify information? Contractors receive their authority from an original classification authority. This is done through the derivative classification process. Contractor personnel who in their official capacity incorporate, paraphrase, restate, or generate classified information from already classified sources may derivatively classify the newly created documents or material.

In order to properly accomplish this process the contractor must have some type of guidance from the original classification authority. In the NISP we refer to three possible sources:

- Classified source material, such as a classified document
- DD Form 254, which is the basic document for providing guidance to the contractor.
- Classification guide, which would contain more detail than a DD Form 254. Sometimes it is not necessary to provide the contractor a guide. The Classification Guide, if needed by the contractor should be provided as an attachment to the DD 254.

## **BASIC DOCUMENT - DD FORM 254**

In accordance with the DD Form 441, Security Agreement, the government has agreed to provide classification guidance to the contractor. This security classification guidance is the responsibility of the program/project manager. The basic document in providing this guidance is the DD Form 254, "DoD Contract Security Classification Specification." Whenever classified information is expected to be received, produced, or accessed by the contractor, a DD Form 254 must be issued (Para. 7-102, ISR). So that it provides comprehensive guidance to the "hands on" person at the facility, it should contain classification, upgrading, downgrading, and declassification instructions regarding the project. Although the DD Form 254 is the basic means of providing classification guidance to the contractor, it may be supplemented by a classification guide for a program or project.

DD Forms 254 are issued as follows:

- Original - With each RFP, RFQ, IFB or other solicitation. With GCA classified programs or projects. Upon award of a classified contract.
- Revised - When the security requirements change.
- Final - When the contractor has a need to retain classified material for more than 2 years after conclusion of contract.

## **CHALLENGES TO CLASSIFICATION**

In accordance with the NISPOM, contractors must establish a procedure to ensure the necessity, currency, and accuracy of the guidance they are provided. Should they question the guidance they are now required to contact the program/project manager for further guidance or clarification.

## **SUMMARY**

Classification is applied only to national security information owned by or under the control of the U.S. Government. The User Agencies through the Security Agreement have agreed to provide classification guidance throughout the acquisition cycle. The "DoD Contract Security Classification Specification," DD Form 254, is the basic document for conveying classification, regrading, and declassification requirements. Classification management must be performed at all levels where classified material is originated, generated, reproduced, or disseminated further. Contractors are responsible for applying the

classification instructions to any material they receive or generate. In order to provide proper protection of the material the principles of derivative classification must be understood and utilized as well as the marking requirements of the NISPOM. Therefore, you, the User Agency must be aware of your responsibilities as they apply to providing proper classification guidance to your contractors. Remember that they are protecting your information.

## REVIEW EXERCISE

Complete the following exercises for review and practice.

1. The Information Security O\_\_\_\_\_ O\_\_\_\_\_ is the government activity responsible for monitoring the information security programs of all executive branch agencies.
2. Information becomes classified information in one of two ways:  
o\_\_\_\_\_ and d\_\_\_\_\_.
3. Contractors receive classification guidance from classified documents, DD Form 254, and classification guides.  
  
True  
False
4. In accordance with the DD Form 441, Security Agreement, the government is obligated to provide classification guidance to the contractors.  
  
True  
False
5. The purpose of the DD Form 254 is to provide c\_\_\_\_\_ guidance to the "hands on" person at the facility.
6. DD Form 254 must be issued with each RFP, RFQ, or any formal solicitation and upon award of a c\_\_\_\_\_ c\_\_\_\_\_.
7. In accordance with the NISPOM, the contractor must establish a policy to ensure the current, n\_\_\_\_\_, and a \_\_\_\_\_ of the guidance they are provided.

## **ANSWERS**

### *Solutions and References*

1. *Oversight Office (p. 4-1)*
2. *originally or derivatively (p. 4-2)*
3. *True (p. 4-2, 3)*
4. *True (p. 4-3)*
5. *classification (p. 4-3)*
6. *classified contract (p. 4-3)*
7. *necessity, and accuracy (p. 4-3)*

## **LESSON 5**

# **Safeguarding Classified Information**

Safeguarding is more than having an approved security container. It is an all-inclusive philosophy encompassing not only physical storage capability, but all other facets of contractors' security programs ranging from the adequacy of the personnel security safeguards to the effectiveness of the security awareness briefings.

Industry is required by contract to comply with the safeguarding requirements of the NISPOM. As you can imagine, how well industry adheres to these requirements impacts upon national security.

At the same time, the responsibility to ensure adequate safeguarding of classified information does not rest solely with the contractors. The User Agencies who have placed classified information into the hands of industry must be aware of, and responsive to, their required participation in the accomplishment of this fundamental NISP function.

## **OBJECTIVES**

At the completion of this lesson you should be able to:

- Determine when and how to accomplish the verification of contractor safeguarding capability.
- Distinguish between level of facility-clearance and level of safeguarding capability.
- Identify the contracting officers' responsibilities toward industry in the areas of reproduction, transmission, and disposition of classified information.

## **THE NISPOM AND THE INDUSTRIAL SECURITY REGULATION**

As you may know, there are numerous differences between the National Industrial Security Operating Manual (NISPOM) and the Industrial Security Regulation (ISR). In fact, many NISPOM requirements have no equivalent requirement in the ISR. Thus, at times, the User Agency is unaware of the requirements with which industry must comply and this often hinders their responsiveness to contractors' requests for guidance or certain authorizations.

## **RELEASE OF CLASSIFIED MATERIAL**

Prior to the release of classified information to a contractor, whether in an RFP, RFQ, some other type of formal solicitation, or the awarding of the contract, the Government Contracting Activity (GCA) must be assured the contractor is properly cleared. As you learned early, there are two ways to verify a facility is in the NISP. First, if your activity currently has a classified contract with them at a higher or equal clearance level. Second, by contacting the Defense Security Service - Central Verification Activity (CVA) at

[www.dss.mil](http://www.dss.mil). in Columbus Ohio. Phone: 1 888-282-7682; or Mailing Address: 2780 Airport Drive, Suite 400, Columbus OH, 43219-2268. If you have the facility's Commercial and Government Entity (CAGE) number, it will aid in determining if the facility is in the program.

Keep several things in mind regarding this verification. It is valid for a period of three years. If any of the information provided to you changes within that time, you will automatically be notified by the CVA". In addition, and most important, a contractor's storage capability may be different than the level of the Facility Clearance. About half of the facilities in the NISP have no storage capability. These facilities are called "Access Elsewhere" facilities. Also note, a facility could be cleared at the TOP SECRET level, but yet only have storage capability at the SECRET level. Never equate clearance level to level of storage capability.

Storage may, however, be required in order to perform on the classified contract. In this case, the contractor is required to obtain the proper container and initiate the proper procedures that will allow DSS to approve the contractor's safeguarding capability. Safeguarding is normally verified through CVA. Just be aware you need to advise the clerk of the volume of classified material you wish to transmit to the facility. You wouldn't want to send ten classified missiles to a facility that has only a two-drawer container. For verification of large volumes of material or classified hardware, contact the Facility Security Officer at the receiving facility.

After you have verified the facility is cleared, be sure to address your material to the address given to you by CVA. This will assure that appropriately cleared individuals handle your material once it reaches the contractor. If the contractor has sent classified materials to your office, be sure to sign and return the receipt. It is the contractor's responsibility to show evidence that the material arrived safely. Should you forget, the contractor will be getting in touch with you regarding the signed receipt.

Keep in mind, you should never send any classified material, including CONFIDENTIAL material by first class mail to the contractor. This may result in an uncleared individual receiving your classified material, since the system that contractors are required to establish for receipt of classified mail only by appropriately cleared personnel covers receipt of classified material by U.S. Registered Mail, U.S. Express Mail, and U.S. Certified Mail only.

## **ACCOUNTABILITY**

Contractors are required to maintain accountability records for TOP SECRET information. For SECRET and CONFIDENTIAL information the contractor has to record when it is received or dispatched outside the facility. Apart from its dispatch, they are not required to account for SECRET and CONFIDENTIAL material generated inside the facility. The NISPOM lists the necessary information required to be maintained in the accountability records.

The contractor is required to obtain written authority from the contracting officer prior to reproducing TOP SECRET information. In the case of COSMIC TOP SECRET, specific written authority from the U.S. or NATO contracting activity is required. At the SECRET level, the information is prohibited from being reproduced if so stated by the contracting officer or originating authority. If it is intelligence community material, check with the customer for approval.

## **TRANSMISSION**

If a facility is going to transmit TOP SECRET material outside of the facility, it first must obtain written authorization from the contracting officer. This, as you would imagine, is to prevent any unnecessary exposure to inherent dangers while in transit. The courier must be briefed and cleared TOP SECRET, or the facility may use the Defense Courier Service. In all other cases, the contractor simply follows the procedures listed in the NISPOM for proper transmission. Basically, SECRET material must be sent by U.S. Registered Mail or U.S. Express Mail. CONFIDENTIAL material may also be sent by U.S. Certified mail. SECRET and CONFIDENTIAL material can also be hand-carried by an employee courier as long as the courier has been properly briefed, is appropriately cleared, and, if the arrangements are made beforehand to store the classified material. NISPOM paragraphs 5-408 & 5-409 provide guidance for the use of commercial carriers for shipment of SECRET and CONFIDENTIAL material.

## **DISPOSITION**

The facility must return to the User Agency the classified material if the bid, proposal or quote was not submitted or was withdrawn within 180 days after the opening date. If the bid, quote or proposal was not accepted, they must dispose of material within 180 days after the notification of non-acceptance. Should the facility be awarded the contract, they must dispose of material upon final delivery of the goods or services, upon completion of the contract, as directed in the contract, or when directed by the contracting officer. The facility does have the option to request retention authority beyond 2 years from the GCA, if they can prove it would be benefit the government to have the contractor retain the classified material. This is done in writing by the contractor as soon as possible. If no response is received from the GCA, the contractor may retain the material for two years from the date of its request. The final disposition option the contractor has is destruction of the material. The contractor is authorized to destroy the material unless the material is COSMIC TOP SECRET (which must be returned to the contracting officer), or unless specific instructions have been provided to the contractor regarding the disposition of the classified material.

Normally the contractor has 24 months to dispose of the material upon completion of a contract. In many cases the material may be destroyed. Disposition may include returning the material to the GCA, sending it to another appropriate and authorized recipient, or destroying it.

Even before a classified bid package is released to industry, the clearance level of the facility and its safeguarding capabilities must be verified. Then, when the contract is issued, the contractor must follow the guidelines established in the NISPOM to ensure the proper protection of the classified information. Your involvement throughout the contract is paramount in making sure the contractor has been provided the proper guidance in meeting these security requirements.

## REVIEW EXERCISES

Complete the following exercises for review and practice. Multiple choice questions may have one or more correct choices.

1. Prior to release of classified information to a contractor's facility the Government Contracting Agency must be assured the facility is p\_\_\_\_\_ c\_\_\_\_\_.
2. A facility's having s\_\_\_\_\_ c\_\_\_\_\_ entails more than its being cleared within the NISP.
3. When storage is required as part of a classified contract, the contractor's safeguarding capability is normally verified through the
  - a. DSS-CVA.
  - b. DISCO.
  - c. OISI.
  - d. DSS Headquarters.
4. Never send CONFIDENTIAL material by f\_\_\_\_\_ class mail to the contractor.
5. Contractors are required to maintain accountability records for all classified material.

True  
False

6. For \_\_\_\_\_ and \_\_\_\_\_ information the contractor only has to record when it is received by the facility and/or d\_\_\_\_\_ outside the facility.
7. TOP SECRET material may never be hand-carried outside the facility by cleared employees.

True  
False

8. Before transmitting TOP SECRET material outside the facility, the facility must obtain w\_\_\_\_\_ a \_\_\_\_\_ from the contracting officer.
9. When a bid, proposal, or quote was not submitted or was withdrawn, the facility must return the classified material to the GCA within
  - a. 30 days after the opening date.
  - b. 60 days after the opening date.
  - c. 90 days after the opening date.
  - d. 180 days after the opening date.

10. The final disposition option of classified materials the contractor has is  
d\_\_\_\_\_.

## **ANSWERS**

1. *properly cleared (p.5-1)*
2. *storage capability (p. 5-2)*
3. *a (p. 5-2)*
4. *first (p. 5-2)*
5. *False (p. 5-2)*
6. *SECRET, CONFIDENTAL  
dispatched (p. (pp. 5-2)*
7. *False (p. 5-3)*
8. *written authorization (p. 5-3)*
9. *d (p. 5-3)*
10. *destruction (p. 5-3)*

## LESSON 6

# Violations and Compromises

The importance of the prompt and accurate reporting of security violations and compromises can not be overstated. The protection of classified material is not an obligation to be taken lightly. NISP contractors are required to educate their employees of their reporting requirements and obligations. Your position as a representative of the government agency you work for is no less demanding. You have the obligation to ensure that your personnel are aware of the reporting requirements and the reasons why it is so important. The lives of the Warfighter depend on it.

### OBJECTIVES

At the end of this lesson you should be able to do the following:

- Explain the reporting requirements levied on the contractor.
- Explain the role of the Defense Security Service upon receipt of the facility's report.
- Identify the responsibilities of the User Agency.

Within each facility the contractor must establish procedures whereby each cleared employee will report to the Facility Security Officer (FSO) any of the following conditions:

- Loss, compromise, or suspected compromise of classified information or material
- All security violations
- Questionable or suspicious contacts
- Espionage, sabotage, or subversive activities

When the employee is outside the facility, he or she must make the report to the local FBI office. An employee who is outside the United States would normally make the report to the nearest U.S. authority.

After receiving the report, the FSO must ascertain all the necessary information regarding the incident in order to answer the questions who, what, when, where, why, and how (W5H). With this information the FSO should be able to analyze the cause, fix responsibility, and take the proper corrective action so as to preclude the incident from recurring.

### REQUIRED REPORTS

The FSO must determine whether or not a report must be filed with DSS. As defined in the NISPOM, a security violation is "failure to comply with the policy and procedures established by this Manual that reasonably could result in the loss or compromise of classified information." Those incidents that result in the loss, compromise, or suspected compromise of classified information, regardless of its classification level, must be reported to the DSS Field Office. Any incident that involves existing or threatened espionage,

sabotage, or subversive activities must be reported to the FBI office, with an information copy going to the DSS Field Office.

## **ADMINISTRATIVE INQUIRIES**

Should the FSO determine that a report must be filed with the DSS Field Office, the preliminary report (containing, as much information concerning the incident as is known at that time) must be sent to DSS promptly upon learning of the incident. If necessary, the final report should be completed when the investigation has been completed. Again, the final report should answer all of the (W5H) questions. It should also identify what corrective action has been taken to make sure the incident does not occur again.

## **DSS ACTIONS**

The primary concern on the part of DSS is to ensure the continued safeguarding of your classified information. Immediate action will be taken if it appears to DSS that safeguarding is inadequate. If necessary, DSS will even conduct its own administrative inquiry at the facility.

DSS establishes the suspense dates for any follow-up actions, and will submit a report to the appropriate contracting officer, who will conduct a damage assessment for the classified information involved.

## **SUMMARY**

Security violations, compromises, and suspected compromises pose threats to the national security. Reasons for their occurrence range from:

- Lack of supervision
- Lack of adequate security education
- Improper security practices
- Human error
- And, at times, poor or hostile attitudes toward security

The contractor is obligated to establish and ensure adherence to procedures whereby each failure on the part of an employee to comply with a requirement of the National Industrial Security Program Operating Manual is immediately reported to the Facility Security Officer. The FSO is in turn responsible to report each violation to the DSS Field Office if the violation resulted in the loss, compromise, or suspected compromise of classified information.

The DSS Field Office makes the final determination in all cases. In order to make a proper judgment, the IS Representative must have available to him/her a thorough administrative inquiry, preferably one conducted by the contractor. Action to ascertain or minimize the damage to the national security is the responsibility of the User Agency.

Finally, instances involving espionage, sabotage, or subversive activities are not matters for investigation by either the contractor or the DSS, but rather must be reported immediately to the FBI.

## REVIEW EXERCISES

Complete the following exercises for review and practice. Multiple choice questions may have one or more correct choices.

1. Within each facility the contractor must establish procedures whereby each c\_\_\_\_\_ e\_\_\_\_\_ will report all security violations to the FSO.
2. An employee who encounters espionage, sabotage, or subversive activities outside the facility must report the incident to the FBI.

True  
False

3. After ascertaining all the necessary information relating to a reported violation the FSO must answer (at a minimum) the following:
  - a. EMC2
  - b. PI2
  - c. W5H
  - d. C4
4. Security violations that resulted in the loss, compromise, or suspected compromise of classified information must be reported to the DSS Field Office.

True  
False

5. The preliminary report must be made to the DSS Field Office promptly upon learning of the incident.

True  
False

6. If necessary, a final report should be completed within 15 days.

True  
False

7. The primary concern on the part of DSS is to ensure the continued safeguarding of the c\_\_\_\_\_ i\_\_\_\_\_ in the contractor's possession.

8. A report of compromise of classified information is submitted by DSS to the appropriate c\_\_\_\_\_ o\_\_\_\_\_ for a damage assessment.

9. Security violations, compromises, and suspected compromises present threats to  
n\_\_\_\_\_ s\_\_\_\_\_.

10. Action to ascertain or minimize the damage to the national security is the  
responsibility of the User Agency.

True

False

## **ANSWERS**

1. *cleared employee (p. 6-2)*
2. *True (p. 6-2)*
3. *c (p. 6-2)*
4. *True (p. 6-2)*
5. *True (p. 6-2)*
6. *False (p. 6-2)*
7. *classified information (p. 6-2)*
8. *contracting officer (p. 6-2)*
9. *National security (p. 6-2)*
10. *True (p. 6-2)*

## LESSON 7

# International Activities

In its relationships with foreign governments, the United States has entered into numerous treaties and agreements whereby each signatory government agrees to safeguard the classified information released to it by the other government. These range from simple bilateral agreements providing for technical assistance to multilateral treaties establishing international organizations for concerted defense. There is an increasing trend toward co-development and co-production of weapon systems. The U.S. Government officially encourages U.S. industry to become increasingly involved in foreign markets. These agreements and policies, treaties and trends all influence the international activities of participants in the National Industrial Security Program (NISP).

## OBJECTIVES

At the end of this lesson you should be able to:

- State the requirement for U.S. contractor facilities to protect classified information from a foreign government.
- Discuss the roles and responsibilities of the employer, the host activity and Defense Security Service in support of U.S. contractor personnel working in support of U.S. Government contracts at foreign locations.
- Define Foreign Military Sales.
- Define Commercial Sale of military articles including classified information.
- Discuss the provisions for granting a Limited Access Authorization

## FOREIGN GOVERNMENT INFORMATION

Foreign Government Information (FGI) is information that is provided to the United States by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both are to be held in confidence. FGI could also include that which is produced by the U.S. pursuant to, or as a result of a joint arrangement with a foreign government or governments or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence.

The U.S. government has entered into agreements with governments of many other countries in which the U.S. government agrees to protect FGI while it is in the United States. This includes that FGI that is in the possession of cleared U.S. contractor facilities. The FGI is assigned an U.S. classification that provides a degree of protection at least equivalent to that required by the entity that furnished the information. U.S. contractors are in turn required to protect the FGI at a level at least equal to the equivalent U.S. classification.

The Cognizant Security Office (CSA) (normally Defense Security Service) administers oversight and ensures implementation of the security requirements of the contract on behalf of the foreign government, including the establishment of channels for the transfer of classified material. Any classified material or information including FGI passing from the United States to a foreign entity must pass through government to government channels.

An U.S. contractor may have possession of FGI related to a contract with the U.S. government or related to a contract with the foreign government or international organization. In either case it is the obligation of the U.S. government to oversee the security procedures in place to protect that information.

Details related to the protection of FGI are found in the NISPOM Chapter 10.

## **OFFICE OF SECURITY SERVICES INTERNATIONAL (OSSI)**

The Office of Security Services International (OSSI) provides industrial security oversight, advice, and assistance to cleared U.S. contractor employees assigned overseas; and provides support in the areas of contractor industrial security and personnel security investigations to U.S. Government activities in the international environment.

The OSSI is also available to facilitate government-to-government transmissions of classified information, act as point of contact regarding accurate and timely communications of personnel security clearance (PCL) information, provide technical support for the Electronic Personnel Security Questionnaire (EPSQ), provide security briefings and assist on international industrial security matters.

Should you have any security questions related to cleared employees located abroad or want to know more about how the OSSI office can assist you, please visit the OSSI page on the DSS internet site ([www.dss.mil](http://www.dss.mil)).

## **U.S. CONTRACTORS AT OVERSEAS LOCATIONS**

Many cleared U.S. contractor employees work at overseas locations in support of contracts with the United States government. This includes contractor personnel who travel for temporary assignments as well as those who are assigned overseas on a long-term basis. The most common example is an employee of an U.S. government contractor who works on an U.S. military installation outside of the United States.

If a cleared contractor employee is assigned to an overseas duty location for over 90 days the employer must report this fact to DISCO. This report should include all personal identifying information, clearance information and information regarding the overseas duty location. It should also include phone numbers and other information that will help the OSSI to locate the employee to provide support, information and services. Contractor employees who are new to an overseas location or who have not had previous contact with OSSI should contact OSSI and advise that office of their location.

If a cleared contractor employee is at an overseas location for an extended period the need for that individual to retain a personnel security clearance must be re-justified every 3 years.

The requirement for adequate security education for cleared employees is particularly important for those who work outside of the United States. Contractors are required to insure that their employees receive security training commensurate with their assignments. Providing this training is a challenge for the company's security office because the employees are located far from the home office. In addition to security training that the company provides to all cleared employees, those on overseas assignments should receive Anti-Terrorism/Force Protection (AT/FP) training. CI/Threat Information relevant to the local area, instructions on handling, disclosure and storage requirements at their duty location, and any other special briefings required by the installation or activity that they are supporting. Depending on their particular duties, they may also need to receive special briefings such as NATO, COMSEC, CNWDI, etc., in accordance with the NISPOM.

It is ultimately the responsibility of the employing facility to ensure that the cleared employees receive appropriate training. In many cases, however, the contractor employees may be included in training that is provided by their host or other U.S. government activities in the area. Outstanding resources and assistance is also available through the U.S. Department of State Regional Security Officer (RSO).

Visit authorization letters to U.S. military and other U.S. Government Activities are sent from the company's home office facility directly to the U.S. activity in accordance with the requirements of NISPOM, Chapter 6, and the procedures of the host activity.

Visits to foreign governments and foreign contractors are initiated by the employing contractor facility and submitted through DISCO to the foreign government. Special procedures are required for visits to NATO facilities. These procedures are detailed in the NISPOM, Chapter 10.

The storage, custody and control of classified information required by contractor employees at overseas locations, is the responsibility of the United States Government. Storage at locations not under U.S. military or other U.S. Government Activity is prohibited. Storage of classified information at overseas divisions and subsidiaries of U.S. companies is prohibited.

Employees assigned to foreign government or foreign contractor facilities under a direct commercial sales agreement are subject to the host-nation's industrial security policies. The Defense Security Service does not have jurisdiction over those facilities.

## **FOREIGN MILITARY SALES**

Foreign Military Sales (FMS) is that portion of U.S. security assistance authorized by the Arms Export Control Act, as amended, and conducted on the basis of formal contracts or agreements between the United States Government and an authorized recipient

government or international organization. FMS includes government-to-government sales of defense articles or defense services, from DoD stocks or through new procurements under DoD-managed contracts, regardless of the source of financing. An U.S. contractor's involvement in an FMS most commonly is selling the goods or services to the U.S. Government who in turn sells it to the foreign government. The export authorization in an FMS case is derived from the "Letter of Offer and Acceptance."

## **DIRECT COMMERCIAL SALES**

A commercial sale (aka: direct commercial sale) is sale of defense articles or defense services made under a Department of State-issued license by U.S. industry directly to a foreign buyer, and which is not administered by DoD through FMS procedures. To apply for authorization for export of classified material the company uses a DSP Form 85. This application is processed through the Department of State, Office of Defense Trade Controls (ODTC). If approved, this form becomes the export license that is the company's authorization to export the articles included in the license.

## **LIMITED ACCESS AUTHORIZATIONS (NISPOM 2-210 & 2-211)**

Only U.S. citizens are eligible for a security clearance. Every effort is made to ensure that non-U.S. citizens are not employed in duties that may require access to classified information. However, compelling reasons may exist to grant access to classified information to an immigrant alien or a foreign national. Such individuals may be granted a Limited Access Authorization (LAA) in rare circumstances. The NISPOM stipulates strict guidance under which a contractor employee may be granted an LAA, and limitations on the type of information that can be disclosed to an individual with an LAA.

## **THE ROLE OF DEFENSE INDUSTRIAL SECURITY CLEARANCE OFFICE (DISCO)**

DISCO supports international activities in a variety of ways. They coordinate with foreign governments to provide and receive security assurances. When appropriate DISCO issues LAAs. DISCO facilitates visit authorization requests from U.S. contractors to foreign entities and provides numerous other services.

## REVIEW Exercises

1. U.S. contractors are required to protect the foreign government information (FGI) at a level at least equal to the equivalent U.S. classification.

True  
False

2. U.S. contractors are required to insure that their cleared employees at foreign locations receive proper security training. In some cases part of this training may be provided by the U.S. military facility where the cleared employees are stationed.

True  
False

3. In a Foreign Military Sales (FMS) case an U.S. company normally sells military articles directly to a foreign government.

True  
False

4. An U.S. company must receive an export authorization prior to shipping classified material to a foreign government.

True  
False

5. Limited Access Authorizations are routinely granted to non-U.S. Citizens and are considered to be equivalent to a SECRET Personnel Security Clearance.

True  
False

# ANSWERS

## Chapter 7. International

1. *True* (p. 7-1)
2. *True* (p. 7-3)
3. *False* (p. 7-3)
4. *True* (p. 7-4)
5. *False* (p. 7-4)

## **LESSON 8**

# **Information Systems Security**

All classified information must be protected at all times. This includes classified information in electronic form. Government classified information processed on contractor information systems must be safeguarded to ensure the information is accessed by authorized persons and the information is used for its authorized purpose.

The Government Contracting Agency (GCA) has the responsibility to provide classification guidance identifying what information is classified. The contractor has the obligation to protect the classified information when processing this data on information systems. A cleared facility processing classified information on an information system must comply with the NISPOM. If contractor employees are users of a government owned information system (for example on a military installation) they must follow the security procedures established for that system. In most cases, within DoD, this will be the Information Technology Security Certification and Accreditation Process (DITSCAP).

### **OBJECTIVE**

At the completion of this lesson you will be able to describe the procedures necessary for a contractor to process classified data on an information system.

### **INTRODUCTION**

Information systems are an integral part of our lives. This technology makes it quick and easy to gain access to information. Just as with classified paper documents, classified electronic data processed on an information system must be protected from unauthorized use and disclosure. Protection measures must be commensurate with the classification level of the information being processed, the identified threats and vulnerabilities, and the system's operating environment.

### **GUIDANCE**

Regardless of the complexity of the accredited system, the contractor must know what information is classified. The classification guide and/or the DD Form 254 identifies the classified elements of the project. Information systems that are used to capture, create, store, process or distribute classified information must be properly managed to protect this classified information. Protection of these systems includes, but not limited to, administrative, operational, physical, communications, and personnel controls. The requirements for protecting classified information that is processed on contractors' information systems are defined in NISPOM, Chapter 8 (Information System Security).

## **ACCREDITATION**

Accreditation is the formal approval from DSS to permit operation of an information system in a specified environment, at an acceptable level of risk, based on the implementation of an approved set of technical and procedural safeguards. The NISPOM requires any information system processing classified information to be accredited to the level of the information being processed. Regardless of whether the information system is a stand alone computer or complex local area network, DSS must inspect the system and approve the security procedures that the contractor will implement before, during, and after classified processing.

The contractor must certify to DSS that the security procedures and protection measures are in place, tested and operational. These security procedures will be documented in a System Security Plan (SSP).

The Industrial Security Representative (IS Rep) will review the SSP and use this document during an inspection of the system. The IS Rep's inspection is to ensure the procedures and safeguards defined in the SSP are adequate to protect the classified data from unauthorized disclosure. A favorable determination results in the issuance of accreditation. Before classified processing can begin, the contractor must receive from DSS written approval that states the information system meets the criteria of the NISPOM, Chapter 8. Upon receipt of written authorization, the contractor can begin classified processing on the accredited system.

## **WITHDRAWAL/INVALIDATION OF ACCREDITATION**

DSS must be notified if changes are made to the accredited system. The IS Rep will evaluate the risks to determine if the approved protection measures identified in the SSP remain effective. If it is determined that the approved procedures become ineffective or changes to the system security configuration become unacceptable, the IS Rep may withdraw accreditation of the information system.

Depending on the severity of the security breach and potential for compromise, accreditation of the system may be invalidated and classified processing terminated. The IS Rep understands the importance to continue uninterrupted classified processing and will work with the contractor to ensure appropriate procedures are being used effectively.

## **RE-ACCREDITATION**

An information system may need re-accreditation if changes are made to security-relevant resources of the information system. Security-relevant resources include: software, firmware, hardware, or interfaces and interconnections to networks. All modifications to security-relevant resources must be reviewed and approved by DSS prior to implementation to determine if the proposed modifications will impact the protections and safeguards on the accredited system. The IS Rep will make a determination if re-accreditation is required.

## **CERTIFICATION & ACCREDITATION OF SIMILAR SYSTEMS**

If two or more similar information systems are operated in equivalent operational environments, a Master SSP may be written. DSS will accredit the first system under the Master SSP. All other systems to be operated under the Master SSP can be certified to process classified information by a designated official within the facility. This designee must be technically knowledgeable of information systems and have specific experience with other similarly configured systems.

## **PHYSICAL SECURITY**

Safeguards must be established that prevent or detect unauthorized modification of the information system hardware and software. Hardware integrity of the information system, including remote equipment, must be maintained at all times, even during periods when the accredited system is not processing classified information. Examples of physical security include: continuous supervision, use of approved cabinets, enclosures, seals, locks or closed areas and use of area controls. This protection ensures that when classified information is introduced into the system, the integrity of these components will not be compromised.

In addition, classified processing shall take place in a DSS approved area. Attended classified processing must take place in an area where authorized contractor personnel can exercise constant surveillance and maintain control of the information system. The area must have an identifiable boundary (e.g. walls, signs, tape on floor, rope or chains) where it is obvious that the area is restricted to only authorized personnel. Unattended classified processing requires a closed area and supplemental controls, which are determined by the accreditation level of the information system. The area established by the contractor must be described in the SSP and approved by the IS Rep prior to processing classified information on the information system.

## **DITSCAP**

Contractor employees assigned to work on an information system that is under the control of the User Agency may be subject to other policies and procedures. An example of this would be the DoD Information Technology Security Certification and Accreditation Process (DITSCAP). This OSD directive presents a standardized approach to the accreditation of information systems that process classified information. DITSCAP must be contractually mandated and remain in effect for the lifecycle of the information system. Note: DITSCAP requirements do not apply to contractor facilities that implement the requirements of NISPOM, Chapter 8. Further information on DITSCAP can be obtained from the Information Assurance Support Environment web site: <http://iase.disa.mil>

## REVIEW EXERCISE

1. The requirements for protecting classified information that is processed on a contractor's information system are defined in:
  - (a) NISPOM, Chapter 5
  - (b) DD-254
  - (c) NISPOM, Chapter 8
  - (d) DISCO Form 562
  
2. Accreditation of an information system authorizes the system to process classified information.

True  
False
  
3. Specific security procedures and protection measures for an accredited information system are documented in:
  - (a) DD-254
  - (b) System Security Plan (SSP).
  - (c) DISCO Form 562
  - (d) Security Agreement (DD Form 441)
  
4. Who has accreditation authority for contractor owned information systems processing classified information?
  - (a) Facility Security Officer (FSO)
  - (b) Facility System Administrator
  - (c) DISCO
  - (d) Defense Security Service (DSS)
  
5. The Contractor must receive written approval from DSS before classified processing can begin.

True  
False
  
6. Changes to security-relevant resources may result in re-accreditation of the system. Who makes that determination?
  - (a) Defense Industrial Security Clearance Office
  - (b) Industrial Security Representative
  - (c) Facility Security Officer
  - (d) Office of the Secretary of Defense

7. One purpose of a Master SSP is to allow the contractor to certify similar information systems that process classified information.

True

False

8. Protection of the accredited system (hardware/software) is not required when the system is powered off.

True

False

## **ANSWER**

1. *c* (p.8-1)
2. *True* (p. 8-2)
3. *b* (p. 8-2)
4. *d* (p. 8-2)
5. *True* (p. 8-2)
6. *b* (p. 8-2)
7. *True* (p. 8-3)
8. *False* (p. 8-3)

## LESSON 9

# Reviews

You will recall that contractors are obligated by their execution of the DD Form 441, "Department of Defense Security Agreement," to preserve and maintain the security of the United States through the prevention of improper disclosure of classified information. This formidable task requires contractor compliance with the requirements of the National Industrial Security Program Operating Manual (NISPOM). As you learned, the NISP is administered through the Defense Security Service (DSS) acting for the Department of Defense and the other User Agencies. DSS reviews the contractor facilities and provides service to User Agencies through evaluation and verification that classified information placed into the hands of industry is being adequately safeguarded.

## OBJECTIVES

At the end of this lesson you should be able to do the following:

- List examples of events that may lead DSS to conduct a security review of a facility.
- State the normal time intervals for key DSS and contractor actions.
- Describe the involvement by the GCA in the areas of pre-review research and unsatisfactory review ratings.

## INITIAL REVIEW

The initial review of a facility is conducted within 60 days of the FCL being issued or within 20 days of receipt of classified material. The first review is to ensure proper implementation of the security requirements and to verify the safeguarding capability of the facility. It usually takes the form of an advice and assistance visit.

## APERIODIC GOVERNMENT REVIEWS

The aperiodic government review is a tool used to assess the effectiveness of the contractor's security systems and to assist the contractor in directing its resources toward the most efficient security solutions.

## FREQUENCY

How often are government reviews conducted at a facility? It all depends. Security reviews are not only conducted based on the passage of time but also other events. Normally there is a 1 year period for possessing facilities and 18 months for non-possessing facilities. Events, which would require that DSS to conduct more frequent reviews, could include:

- New counterintelligence information indicating a new or increased threat to the facility or its technologies

- Changes in the scope of the facility's classified operations
- The departure of the FSO
- User Agency concerns major or repeated security violations indicating classified information is in jeopardy
- The introduction of FOCI or significant changes to current FOCI, foreign nationals visiting or assigned to the facility
- And significant international involvement, to name a few.

## **REVIEW TECHNIQUES**

Depending upon the size and complexity of the facility, one or more IS Reps may conduct the review. The time required conducting a review range from several hours for a small access facility to several days for a large facility, particularly those who possess TOP SECRET, COMSEC, and other highly sensitive material.

Under a recent change, the DSS will attempt to contact the program manager at the GCA before the review. The IS Rep will inquire about various aspects of the contract with the FSO, such as the release of classified hardware and classified visits. In this way, the IS Rep has a better understanding of the activity at the facility prior to arriving for the review.

When the IS Rep arrives at the facility, an entrance briefing is conducted with upper management. The IS Rep discusses the upcoming review with management and briefs them on the areas the IS Rep will look at during the review.

## **COMPLETION OF THE REVIEW**

At the completion of the review the IS Rep conducts an exit briefing with the FSO. The IS Rep discusses each problem area with the FSO. Following this briefing, the IS Rep will provide an overview of the review results to top management. If necessary, a follow-up letter will be sent to the facility listing those areas that were not corrected during the review. The facility normally has 30 days to correct these areas.

The GCA is normally not contacted regarding the results of the review. It will be contacted, however, should the facility receive an "unsatisfactory" rating. This rating is given to a facility that is unwilling or unable to adequately safeguard classified information. The GCA then decides whether or not the facility will continue to perform on current classified contracts.

No new classified contracts should be awarded until the "unsatisfactory" conditions have been corrected. DSS will continue to work with the facility during this period in an attempt to correct the problems, which resulted in the "unsatisfactory" rating.

## **SUMMARY**

Contractors are entrusted with the protection of classified information from unauthorized disclosure, and the DSS is entrusted to verify this protection through the security review process. Industrial security reviews are conducted to assist industry in fulfilling the NISP requirements. It is therefore the uniform application of these requirements, the conduct of quality of the in-depth reviews, and the timely exchange of information between activities, that the GCA is assured that their classified information within industry is adequately safeguarded.

## REVIEW EXERCISES

Complete the following exercises for review and practice. Multiple choice questions may have one or more correct choices.

1. An initial review of a cleared facility is normally conducted within 60 days of the FCL being issued. However, should the facility receive classified material within that time period the DSS Field Office will inspect the facility within:
  - a) 15 days
  - b) 20 days
  - c) 30 days
  - d) 45 days
  
2. List three events that may cause DSS to conduct a security review of a facility.
  - a.
  
  - b.
  
  - c.
  
3. The contractor within should correct problems cited in review follow-up letter:
  - a. 10 days
  - b. 15 days
  - c. 30 days
  - d. 60 days
  
4. The User Agency will always be notified when a facility receives an "unsatisfactory" review rating.

True  
False
  
5. An "unsatisfactory" review rating is given when a facility:
  - a. Has no classified contracts
  - b. Is unable or unwilling to safeguard classified information
  - c. Is unable to facilitate an unannounced review
  - d. None of the above

## **ANSWERS**

1. *b (p. 9-1)*
2. *Any three of the events listed on p. 9-1, 2. (p. 9-1, 2).*
3. *c (p. 9-2)*
4. *True (p.9-2)*
5. *b (p. 9-2)*

# Index

	<b>Pages</b>
Access	1-1
ACDA classified information	2-4
Administrative inquiry	6-2
Adverse information	2-4,5,16
Authorized person	2-1; 8-9
Becker v. Philco	2-16
Board of directors	1-5
Bureau of Customs	2-6
Business structures	1-6
CAGE (Commercial & Gov't. Entity) code.	3-2; 5-1
Central Intelligence Agency (CIA).	2-6, 9
Certificate Pertaining to Foreign Interests.	1-1,4,5
Changed conditions	1-7, 8
Classified contract.	1-1, 2,4,5,7; 4-3, 5-1, 2; 9-2
Classified information.	7-1, 2, 3, 4; 8-7,8,9; 9-1, 3
Classified meetings. See meetings.	
Classified visits. See visits.	
Clearances. See facility security clearance (FCL) and personnel security clearance (PCL). See <i>also</i> limited access authorization (LAA).	
Coast Guard	2-6
COMSEC	2-4
CONFIDENTIAL.	2-4,6,9; 4-1; 5-2,3
CONFIDENTIAL information.	2-5; 5-2
COSMIC TOP SECRET	5-2, 3
Certificate Pertaining to Foreign Interests (DD Form 441s).	1-2,4,5; 2-1; 4-2,3; 9-1
DD Form --, See forms.	
Defense Clearance and Investigations Index (DCI 1).	2-4,6
Defense Courier Service.	5-3
Defense Industrial Security Clearance Office (DISCO).	1-1,2,6,8; 2-5,10,11,13,14,15; 3-2; 7-2,3,4
Defense Office of Hearings and Appeals. (DOHA).	2-11,12,13,14,15
Denial of PCL.	2-13
Department of State.	7-3, 4
DISCO Form ---. See forms.	
DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM).	1- 1,2,3,4,6; 2-2,15; 3-1,3,5; 4-2,3; 5-1,2,3; 6-1; 7-2,3,4; 8-7,8,9; 9-1
DoD Directive 5200.1, DoD Information Security Program.	4-2
DoD Directive 5200.2, DoD Personnel Security Program.	2-5
DoD Directive 5220.6, Defense Industrial Personnel Clearance Review Program.	2-12
DOE Form ---. See forms.	

Dormant facility.	1-8
Executive Order 10450.	2-5
Executive Order 10865.	2-12
Executive Order 12958.	4-1
Facility	1-1,2,3,4,5,6,7,8; 2-10,11,14; 3-2,3,4; 4-2,3; 5-1,2,3; 6-1,2; 7-3; 9-1,2
Facility security clearance (FCL).	1-1
Facility Security Officer (FSO).	1-3,6; 2-13; 6-1,2; 9-2
Federal Bureau of Investigation (FBI).	2-6,9; 6-1,2
Foreign national.	1-3; 2-4; 7-4,6; 9-2
Foreign ownership, control, or influence (FOCI).	1-3,4,5,6,7; 9-2
Forms.	
DID Form 254..	4-1,2,3; 8-7
DD Form 441.	1-2,4,5; 2-1; 4-2,3; 9-1
DOE Form 5631.20.	3-4
General Services Administration (GSA).	1-6; 4-2
Home office facility (HOF).	1-5
Immigrant alien.	2-4; 6-9; 7-4
Immigration and Naturalization Service (INS).	2-6,9
Industrial Security Representative (IS Rep).	1-1,3,8; 8-8,9; 9-2
Industrial Security Regulation (ISR). See DoD Regulation 5220.22-R.	
Information Security Oversight Office (ISOO).	4-1,2
Interim	1-2; 2-4,5
Internal Revenue Service (IRS).	2-6
ISOO Directive	4-2
KMP clearances.	1-1
Letter of Notification of Facility Security	1-7
Letter of Consent (LOC) (DISCO Form 560)	2-11,13,14.
Limited Access Authorization (LAA).	2-4,5,6,9; 7-4
Loss.	6-1,2
Meetings (classified).	3-4, 5
Multiple Facility Organization (MFO).	1-5, 6
Military Personnel Records Center (MPRC).	2-6, 9
National Agency Check and Credit Check (NACC).	2-9
Industrial Security Program. (NISP).	1-1,5,7; 2-1,5,10,11; 3-1,2; 4-1,2; 5-1,2; 6-1; 7-1; 9-1,3
National Industrial Security Program Operating Manual (NISPOM). See DoD 5220.22-M.	
NATO.	2-4,5; 5-2; 7-3
Office of Personnel Management (OPM).	2-6, 9
Organization.	1-1,3,4,5,6; 2-6, 12; 4-1; 7-1,2,3
Parent-subsidiary relationship.	1-5
Partnership.	1-6
Personnel Security Clearance -(PCL).	1-3,6; 2-1,2,10,12; 7-2,3,5
Personnel Investigations Center (PIC).	2-6,11,13,14
Privacy Act of 1974.	2-10; 3-2
Report of investigation (ROI).	2-11
Reproduction.	5-1, 2.
Restrictions.	2-4; 3-1

Reviews.	1-3,8; 2-11,14; 9-1,3
exit briefing.	9-2
SECRET.	1-2; 2-4,5,6,9; 4-1; 5-2,3;
Security education.	2-15; 4-2; 6-2; 7-3
Security Agreement (DD Form 441).	1-4,5; 4-2
Security violations.	1-3; 2-3; 6-1,2; 9-2
SENSITIVE COMPARTMENTED INFORMATION (SCI)	2-4,6,9,11
Single Scope Background Investigation (SSBI).	2-5,6,7,8,9,11
Sole proprietorship.	1-6
Sponsorship.	1-1,2; 3-5
Storage capability.	3-3; 5-1,2
Subsidiary.	1-4,5,6
Suspected compromise.	6-1, 2
TOP SECRET information.	2-4,5,6,8,9,11,16; 4-1; 5-2,3; 9-2
Taglia v. Philco.	2-15
Termination.	1-1,3,7; 2-3
User Agency (UA).	1-1,2,4,8; 2-4; 3-1,3,4,5; 4-3; 5-1,3; 6-1,2; 8-9; 9-2
U.S. Registered Mail.	5-2,3
U.S. Certified Mail.	5-2,3
Visitor Group Agreement.	1-8
visitor group.	1-8

## **Other Online Independent Study Courses Available:**

### **Independent Study Enrollment Information**

**Acquisition Systems Protection Program (DS 6100)**

<http://www.atsc.army.mil/accp/dlsd.htm>

**Basic Industrial Security For User Agency Personnel (IS001.08)**

<http://www.dss.mil/training/indpstud.htm>

**Basic Information Security Independent Study (IF001.08) formerly DISI 3121**

<http://www.dss.mil/training/indpstud.htm>

**Essentials of Industrial Security Management (IS002.08) formerly DS 2123**

**Protecting Secret and Confidential Documents (IS003.08) formerly DS 2124**

<http://www.dss.mil/training/indpstud.htm>

**DoD Personnel Security Adjudication Independent Study PS001.08**

<http://www.dss.mil/training/indpstud.htm>.

**These Online Courses are available through the Defense Security Academy**

**Defense Security Service Academy**

**938 Elkridge Landing Road**

**Linthicum, MD 21090**

**Registrar (410) 865-2295; DSN 283-7295**

**FAX (410) 865-2704**

**Or Visit us online at <http://www.dss.mil/training.htm>**

# **BASIC INDUSTRIAL SECURITY for USER AGENCY PERSONNEL**



**IS001.8 Revision 1**