



EDITION E

Essentials of Industrial Security Management

Course IS002.08

The Cutting Edge



Defense Security Service Academy

The Instructors at the Defense Security Service Academy (DSSA) are committed in providing timely responses to your questions or concerns.

Use the following guidance to help you. E-mail, phone, or fax your questions/ concerns to the appropriate location.

ANY ADMINISTRATIVE QUESTIONS/CONCERNS

PERTAINING TO THE FOLLOWING:

- Enrollment Procedures
- Disenrollment
- Receipt of Course Material
- Course Reissue
- Enrollment Extension

OR CHANGES IN:

- Address
- Contractor Status
- Student ID or Social Security Number

PLEASE CONTACT:

THE DSSA Customer Service Center :

E-MAIL: call.center@mail.dss.mil

TELEPHONE: (888) 347-5213 or (410) 865-3080

FOR SUBJECT MATTER EXPERTISE

PERTAINING TO:

- Confusing Information
- Course Difficulty
- Course Content (inclusive of final examination)
- Missing Course Material
- Interpretation of Course Content/Material

E-MAIL: www.dssa.is@mail.dss.mil

NOTICE

We have made every effort to ensure that the content of this course agrees with the requirements of the *National Industrial Security Program Operating Manual (NISPOM)* in effect at the time of course publication. Because, changes to the *NISPOM* may occur after that time. Please direct any questions regarding technical accuracy to your DSS Field Office. However, when taking the examination at the end of the course, be sure to base your responses to the questions in the course examination solely on the information provided in the course and not on any other source.

January 2004



Defense Security Service Academy
938 Elkridge Landing Road
Linthicum, MD 21090

Welcome to (*Essentials of Industrial Security Management*)

If you are a newly appointed Facility Security Officer (FSO), you may be feeling somewhat uneasy and have some genuine concerns about what is expected of you. You probably feel overwhelmed with the definitions, acronyms, requirements, reports, and forms that seem to have all descended upon you at the same time. If you are like many of your colleagues, other FSOs of small to medium size firms, you may very well have other major duties at your facility, and security may be but one of several hats you wear.

If one or more of these circumstances describe you or your situation, then this course is for you. *Essentials of Industrial Security Management* takes you in a simple and straightforward manner, topic-by-topic, through the baseline requirements for all facilities cleared under the National Industrial Security Program (NISP). And it's written specifically for you - the Facility Security Officer.

Because the NISP relies ultimately on the integrity, knowledge, and willing cooperation of the people who work with classified information on a day-to-day basis, much depends on your success as an FSO. I hope you will find that *the Essentials of Industrial Security Management Course* prepares you to succeed.

Kevin Jones
Director DSS Academy

SAFEGUARDING THE UNITED STATES OF AMERICA

As you spend time studying the material in this course, *Essentials of Industrial Security Management*, it is important that you understand and remember where you fit in to the big picture. As a Facility Security Officer (FSO) or security staff member of a cleared facility you play a very important role in protecting the security of the United States.

Think for a moment of the many freedoms and rights that we enjoy in the United States. The government of the United States is “of the people, for the people, and by the people.” One of the primary functions of this government is to protect its citizens. A strong national defense and effective security programs are vital components, which provide for this protection.

As you perform your duties as a security professional, please keep in mind that you have an awesome responsibility to protect the classified information entrusted to your facility by the U.S. Government. Remember that many foreign governments would like to acquire whatever goods or services your company provide(s) to the U.S. Government. In some cases they may do so by legal means. In many cases, however, foreign governments and terrorist organizations attempt to illegally acquire the information that you are obligated to protect.

Our adversaries use many means to obtain our classified information. Over past decades, the United States has lost vital technology as a result of U.S. citizens selling classified information to foreign entities. We are also aware of many instances when our adversaries simply request that information be given to them. These requests may come in the form of e-mail messages, phone calls, or personal contact with cleared employees. Foreign intelligence services and terrorist organizations are also known to use a variety of other methods to collect information. Any unauthorized disclosure of classified information will cause damage to the United States. Your job, as a security professional is to insure that classified information is protected from any unauthorized disclosure.

This course covers the provisions of the National Industrial Security Program (NISP). The NISP is designed to protect classified information while it is in the hands of U.S. industry. The NISP includes over 11,000 cleared defense contractor facilities ranging in size from giants to one-person operations. There are over 800,000 individuals with security clearances employed by these facilities. An estimated 11 million classified documents are entrusted to industry as well as a huge amount of data in electronic form. The goal of the NISP is to assure that classified information released to industry is properly safeguarded.

As you complete this course and proceed in your duties as a security professional please keep the big picture in view. Take seriously the responsibility that you have to protect the classified information that you and your company’s employees have access to. Use what you learn from this course to properly safeguard classified information according to the provisions of the NISP.

Good luck to you, and enjoy the *Essentials of Industrial Security Management* course.

Contents

	Page
Notice	i
Welcome Letter	ii
Safeguarding the United States	iii
Table of Contents	iv
General Information.....	v
Acronyms and Abbreviations.....	ix
Introduction.....	xi
1 Overview of the National Industrial Security Program	1-1
2 Overview of the National Industrial Security Program Operating Manual.....	2-1
3 The Facility Security Clearance.....	3-1
4 Personnel Security Clearances: General Concepts	4-1
5 Personnel Security Clearance Procedures.....	5-1
6 Reports.....	6-1
7 Procedures for Visitors	7-1
8 Security Education: Briefings	8-1
9 Security Reviews.....	9-1

General Information

PURPOSE

This course is designed to orient Facility Security Officers (FSOs) of facilities cleared under the National Industrial Security Program (NISP) with their basic responsibilities. Members of the FSO's security staff, Defense Security Service employees and User Agency personnel who wish to gain a better understanding of the role of the FSO within the NISP are also encouraged to enroll.

ENROLLMENT ASSISTANCE



On any matter concerning your enrollment (a change in your mailing address, non-receipt of materials, your exam score, etc.) communicate with DSSA. To contact DSSA by telephone, use these numbers.

- Commercial: (410) 865-3080 or (888)347-5213
- DSN: 283-7295/7732
- E-MAIL: dssa.registrar@mail.dss.mil

ADDITIONAL DSS ACADEMY SUBCOURSES

Course descriptions are provided on our website at <http://www.dss.mil/training>, under the homepage for the DSS Academy.

STUDYING THE LESSONS

To get the most out of each lesson we urge you to follow this procedure: Read the lesson objectives and refer to them from time to time as you go through the lesson text. Complete the review exercises for the lesson. Refer to the lesson text to check your answers.

CONTENT ASSISTANCE

If you have a question about the content of this subcourse, a correction or suggestion to improve its content, refer to the administrative questions/concerns page. Our address is:

**DSS Academy
ATTN: Industrial Security Team
938 Elkridge Landing Road
Linthicum, MD 21090**

- Telephone (410) 865-3080 or (888) 347-5213
- Send a fax to **410-865-3221**
- E-mail address: call.center@mail.dss.mil

TIME LIMIT

The National Industrial Security Program Operating Manual (NISPOM) requires that a facility security officer (FSO) complete training "within one year of appointment to the position of FSO." If you are employed by the Defense Security Service and your enrollment has been directed by a supervisor, the course may be completed during duty hours.

COURSE OBJECTIVES

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

- State the purpose of the National Industrial Security Program (NISP) and describe the roles of Government Contracting Activities (GCAs), cleared contractors, and the Defense Security Service (DSS) within the DoD implementation of the NISP.

- Apply key provisions of the National Industrial Security Program Operating Manual in carrying out the duties of an FSO.
- Explain what a facility security clearance (FCL) is, its purpose, and the considerations on which it is based; take appropriate action if changes regarding the FCL occur.
- Explain what a personnel security clearance (PCL) is, its purpose, and the considerations on which it is based. Conduct the initial processing of various applicants for PCLs. Conduct the initial processing of a non-U.S. citizen who is an applicant for a limited access authorization (LAA). Follow procedures for processing changes affecting PCLs and LAAs.
- Prepare and submit timely, accurate reports as required.
- Differentiate the types of classified visits, and apply the procedures associated with them.
- Differentiate various types of briefings and present them as appropriate.
- Differentiate various types of surveys and reviews conducted within the NISP, and respond to findings associated with them as required; conduct a facility self-inspection at a non-possessing facility.

EXAMINATION



When you feel confident that you can meet the objectives for the entire course, do the following:

- Access the ENROL web site:
<https://enrol.dss.mil/enrol/default.asp>
- Go to this course
- And click on the exam URL.

The examination is an open book test; passing score is 75 percent (at least 33 items correct out of 44). If you score less than 75 percent, take the test again.

DSS ACADEMY CERTIFICATE

When you have successfully completed the exam, an online Certificate of Completion will be available for printing.

Go online to: <https://dssaots.dss.mil/cgi-bin/OnlineTest/list.cert.pl>

- Type in your user name that you used to take the exam
- The OTS will display all successfully passed exam grades, date taken, and the certificate. Print the certificate.

Acronyms & Abbreviations

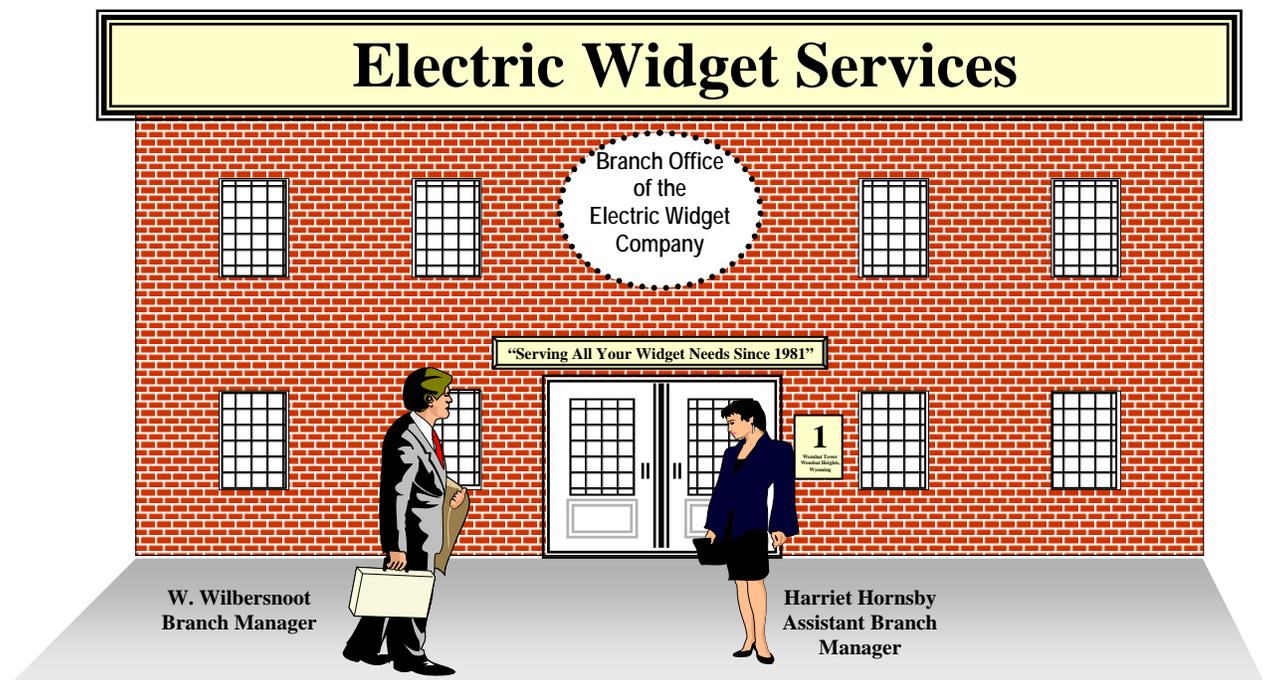
C, (C)	CONFIDENTIAL
CAGE	Commercial and Government Entity
CIA	Central Intelligence Agency
CNWDI	Critical Nuclear Weapon Design Information
COMSEC	Communications Security
CSA	Cognizant Security Agency
CSO	Cognizant Security Office
CVA	Central Verification Activity
DA	Department of the Army
DD	Department of Defense (as in DD Form)
DISCO	Defense Industrial Security Clearance Office
DoD	Department of Defense
DSSA	Defense Security Service Academy
DOE	Department of Energy
DOHA	Defense Office for Hearings and Appeals
DSS	Defense Security Service
EWC	Electric Widget Company (fictional)
EWS	Electric Widget Services (fictional)
FBI	Federal Bureau of Investigation
FCL	Facility Security Clearance
FIS	Foreign Intelligence Services
FL	Form Letter
FOCI	Foreign Ownership, Control, or Influence
FSC	Federal Supply Code
FSO	Facility Security Officer
GCA	Government Contracting Activity
HOF	Home Office Facility
IS	Information Systems
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer

ISSP	Information Systems Security Professional
IS Rep	Industrial Security Representative
ISSR	Information System Security Representative
KMP	Key Management Personnel
LAA	Limited Access Authorization
LOC	Letter of Consent (An electronic transmission from DISCO that indicates date of PCL)
MFO	Multiple Facility Organization
NACLC	National Agency Check with Local Agency Checks & Credit Check
NATO	North Atlantic Treaty Organization
NISP	National Industrial Security Program
NISPOM	National Industrial Security Program Operating Manual
NRC	Nuclear Regulatory Commission
PCL	Personnel Security Clearance
PIC	Personnel Investigation Center
PMF	Principle Management Facility
PSI	Personnel Security Investigation
RFI	Representative of a Foreign Interest
S, (S)	SECRET
SPP	Standard Practice Procedures
TS, (TS)	TOP SECRET
UA	User Agency
VAL	Visit Authorization Letter

Introduction

BASIC SECURITY MANAGEMENT

In this module, we will examine the role that you, the Facility Security Officer (FSO), play in maintaining our national security. In order to make the concepts we're trying to teach more concrete, we'll be visiting the fictitious offices of Electric Widget Services from time to time. Electric Widget Services (EWS) is a small branch office of the Electric Widget Company. Unlike its home office, EWS is not very deeply involved with the handling of classified information. Like many of you out there, EWS is an *access elsewhere* facility. That is, its employees only have access to classified information at sites other than EWS. EWS does not produce or store anything classified.

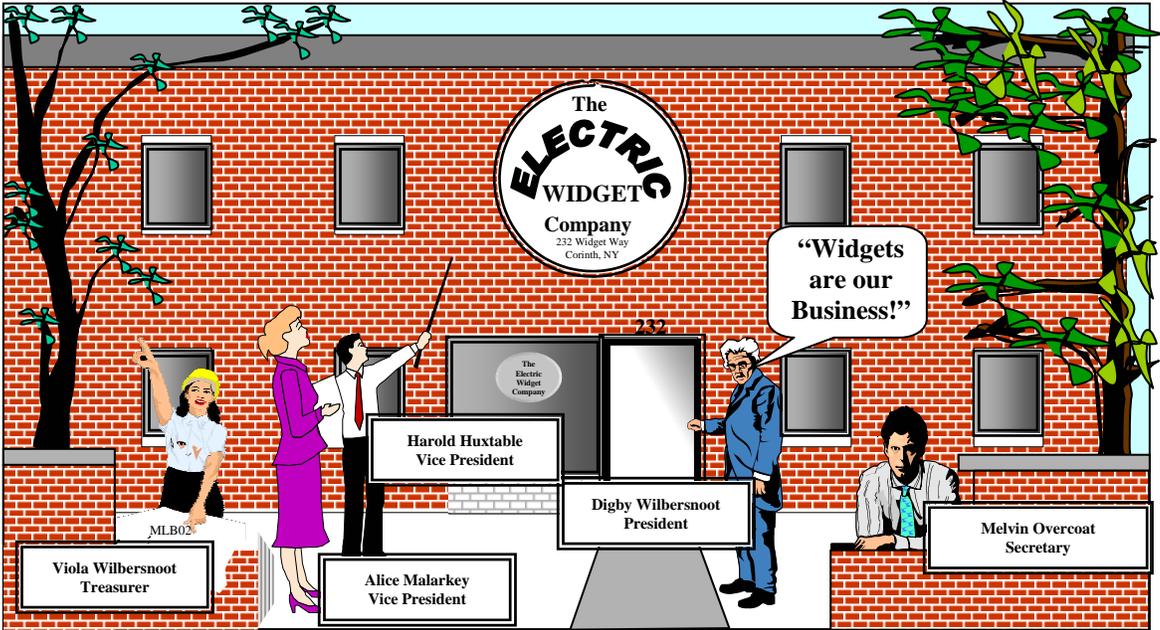


EWS shares the problems and concerns of non-possessing facilities throughout the National Industrial Security Program (NISP).

You should find that most of the security matters at EWS mirror those at your facility. For those facilities with more involvement in the NISP, we will be going to the home office, Electric Widget Company, in our next module.

You will find, on these pages, an illustrated introduction to the people and facilities we will be dealing with. Don't bother with trying to remember any of these details, you'll be introduced to the characters and situations as you go along.

Before we visit EWS, let's look at just what this program for the protection of classified information is and how EWS and your facility fit into it.





SALUS POPULI SUPREMA LEX.

The Safety of the people is the highest law.

—Cicero

LESSON 1

Overview of the National Industrial Security Program

When one stops to consider that nearly 90% of all U.S. classified information originates within the industrial environment, the impact of industry on the national security can scarcely be overemphasized. The National Industrial Security Program (NISP) is a partnership between the federal government and private industry to safeguard classified information. As a Facility Security Officer (FSO), you will be required to ensure that your firm adheres to the policies, practices, and procedures of the NISP. So it is essential that you have a clear understanding of the overall organization, mission, and functions of the NISP, as well as those of the Defense Security Service (DSS), which oversees the NISP for the Department of Defense and works with you, the FSO, in carrying out your duties.

OBJECTIVES

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

- Identify the four Cognizant Security Agencies within the NISP.
- State the purpose of the NISP.

- Identify the roles of Government Contracting Activities (GCAs), cleared contractors, and the Defense Security Service (DSS) within the NISP.
- Define "classified information."
- Recognize the Facility Security Officer's role and responsibilities in the NISP.
- Identify the main elements of the Defense Security Service (DSS) in its administration of the NISP for the Department of Defense.

THE GOVERNMENT-INDUSTRY RELATIONSHIP

The government, especially the military, has a great and pressing need for state-of-the-art technology: weapons systems, information technology, communications systems, and so forth. With rare exceptions, the government does not research, develop, or manufacture these items. Instead, it relies on industry. It also relies on industry for ordinary supplies and support services that in some cases require access to areas containing classified information. In order for industry to meet the government's need it must have access to classified information. This is where the *National Industrial Security Program (NISP)* comes in.

PURPOSE OF THE NATIONAL INDUSTRIAL SECURITY PROGRAM

The NISP is a government-industry team program *to safeguard classified information entrusted to industry*. The government sets requirements for the protection of classified information in the hands of industry, and industry implements these requirements with government advice, assistance, and oversight. Four federal agencies, the *Cognizant Security Agencies (CSA)*, provide these services:

- Department of Defense (DoD)

- Department of Energy (DOE)
- Nuclear Regulatory Commission (NRC)
- Central Intelligence Agency (CIA).

The DoD has delegated the security oversight and the administration of its classified activities and contracts to the *Defense Security Service (DSS)*.

For most security matters you will be dealing directly with two elements of DSS: Defense Industrial Security Clearance Office (DISCO) and the *DSS Field Office (FO)* for your area. We'll have a lot more to say about your relationship with DISCO and the FO as we go along.

CLASSIFIED INFORMATION

Protection of classified information is what the NISP is all about. You need to understand what classified information is so that you can fulfill your duties as an FSO in protecting that information and instructing others in its protection.

Classified information is *official government information which has been determined to require protection against unauthorized disclosure in the interest of national security and which has been so identified by being marked TOP SECRET, SECRET or CONFIDENTIAL.*

These three categories pervade all aspects of the NISP. They form the basis for the handling and safeguarding requirements for classified information. All facilities and all cleared personnel within the NISP are cleared at one of these levels. The classification categories are as follows:

CONFIDENTIAL

Classified information or material which requires ***protection***, the unauthorized disclosure of which could reasonably be expected to cause ***damage*** to the national security that the original classification authority is able to identify or describe. An example of "damage" would be the compromise of information that indicates the strength of our armed forces, or disclosure of technical information about our weapons, such as performance characteristics, test data, design, and production data.

SECRET

Classified information or material that requires a ***substantial degree of protection***, the unauthorized disclosure of which could reasonably be expected to cause ***serious damage*** to the national security that the original classification authority is able to identify or describe. Wrongful disclosure of SECRET information could lead to a disruption of foreign relations significantly affecting national security; could significantly impair a program or policy directly related to national security; could reveal significant military plans or intelligence operations, or compromise significant scientific or technological development relating to national Security.

TOP SECRET

Classified information that requires the ***highest degree of protection***, the unauthorized disclosure of which could reasonably be expected to cause ***exceptionally grave damage*** to our national security that the original classification authority is able to identify or describe. Wrongful disclosure of TOP SECRET information could lead to war against our nation or its allies; could disrupt vital relations with other countries; could compromise our vital defense plans or our cryptologic and communications intelligence systems, reveal sensitive intelligence operations, or could jeopardize a vital advantage in an area of science or technology.

Always be aware that unauthorized disclosure of *any* classified information can cause damage to the national security. Don't fall into the trap of thinking of some classified information as "only CONFIDENTIAL." Different degrees of safeguarding are required for the three levels, but all three types of information *must be protected*.

COMPONENTS OF THE NISP (DoD)

For DoD, the NISP has three main components:

- ***User Agencies, in the role of a GCA.***
- ***Cleared contractors.***
- ***Defense Security Service. In the role of the Cognizant Security Office (CSO) on behalf of the Department of Defense, which is the Cognizant Security Agency (CSA).***

USER AGENCIES

USER AGENCIES
Department of Defense
Department of State
Department of Commerce
Department of Treasury
Department of Transportation
Department of the Interior
Department of Justice
Department of Agriculture
Department of Labor
Federal Reserve System
General Services Administration
Small Business Administration
U.S. Trade Representative
U.S. International Trade Commission
National Science Foundation
Environmental Protection Agency
General Accounting Office
Federal Emergency Management Agency
National Aeronautics and Space Administration
U.S. Arms Control & Disarmament Agency
U.S. Agency for International Development
Nuclear Regulatory Commission
Department of Health and Human Services
Department of Education

Your facility became a part of the National Industrial Security Program at the request of a User Agency or of a cleared contractor to a User Agency. *A User Agency is a federal agency that has entered into an agreement with the Secretary of Defense, the Executive Agent for the NISP, for industrial security services.* The User Agencies are government customers of private industry. The Air Force, the Army, the Navy, in fact, *all* Department of Defense (DoD) components are User Agencies. There are also 24 non-DoD departments and agencies that are User Agencies.

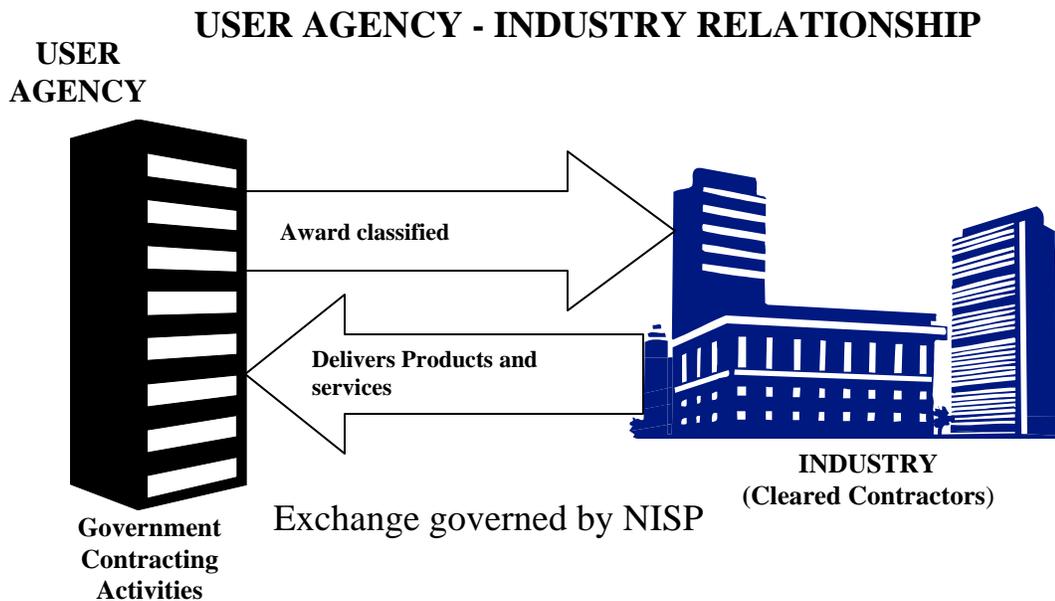
Each User Agency has one or more Government Contracting Activities (GCAs). *A GCA is an element of a federal department or agency that is designated to handle acquisitions for that department or agency.* Experts at GCAs of the User Agencies determine when one of their contracts will involve classified information. They then identify in the contract the kinds of classified information to which the contractor will require access. If the contractor will be generating material or information that is classified, the GCA will provide guidance to the contractor (incorporated in the contract) as to what information is classified and at which level. Note that the User Agency, not the contractor, owns the classified information.

NOTE: The DOE, NRC and CIA each have procedures for oversight and administration of the NISP for contracts involving these agencies. Those procedures are not covered in this course.

CLEARED CONTRACTORS

All work performed by industry for the U.S. Government is performed under contract. If classified work or products are involved, it is necessary to "clear" the contractor (the private industrial firm involved). This clearance, called a *Facility Security Clearance (FCL)*, is an administrative determination made by the government that the facility is eligible for access to classified information.

There are about 11,000 cleared contractors in the NISP, ranging in size from industrial giants such as Boeing, Northrop Grumman and Lockheed Martin to the many smaller firms and one-person businesses. About half of all cleared contractors possess classified material at their own facilities. The other half, most of which are service organizations, do not possess classified material. Instead, their employees have access to classified information at the possessing facilities or at User Agency installations.



Cleared contractors employ 800,000 cleared employees. There are over 11 million classified documents entrusted to cleared contractors.

So far, we have seen that there is a mutually beneficial relationship between government and industry. The government receives essential goods and services, and industry profits from the exchange. User Agencies are federal government agencies that need goods and services that involve classified information, and industrial firms become cleared contractors as a result of that need. Let's turn now to the third component of the NISP for DoD: the Defense Security Service (DSS). We said that the DoD has delegated security administration of its classified activities and contracts to DSS. In this role, DSS is sometimes referred to as the "Cognizant Security Office" (CSO) within the DoD. By their agreements with the Secretary of Defense, the heads of the other User Agencies authorize DSS to administer the security measures for their classified activities and contracts. How did the DSS come to play this important role?

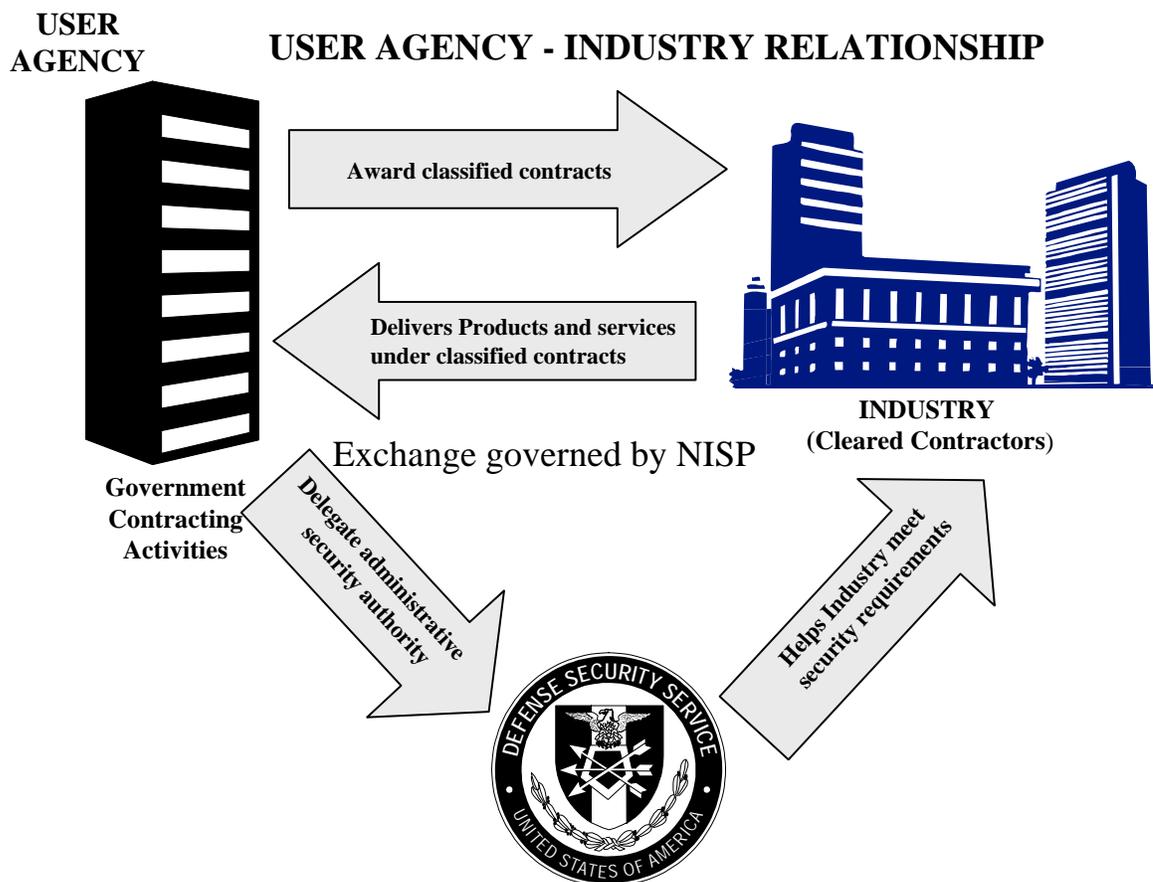
DEFENSE SECURITY SERVICE



For many years, until around the time of the Korean War, the agencies that are now the User Agencies administered their own security programs. Then, to provide greater uniformity in the handling of classified information, the Defense Industrial Security Program (DISP) was formed. The uniformity simplified the handling of classified information for industry. Rather than having to comply with separate security rules and regulations set by each government agency for each contract, there was only one set of rules for all contracts awarded within the DISP. To achieve even greater uniformity in the security requirements for classified contracts, the National Industrial Security Program (NISP) was launched in 1993. Now the Department of Energy, the Nuclear Regulatory Commission, and the Central Intelligence Agency have joined with the Department of

Defense in subscribing to a single set of rules for their classified contracts: The National Industrial Security Program Operating Manual (NISPOM).

The administration of the DISP was undertaken initially by the individual military services. In 1965 the DISP was placed under the centralized management of the Defense Logistics Agency (DLA). The Defense Investigative Service (DIS) was established in 1972 and in 1980 replaced DLA as the administrative agency for the DISP. With the creation of the NISP in 1993, the Secretary of Defense designated DIS the Cognizant Security Office (CSO) for DoD. In 1997, DIS was renamed the Defense Security Service (DSS). The Director, DSS, administers the NISP on behalf of the Secretary of Defense and the User Agencies.



ROLE OF THE FACILITY SECURITY OFFICER IN THE NISP

We now have the three components of the NISP for DoD: User Agencies, cleared contractors, and the Defense Security Service. As the *Facility Security Officer (FSO)* for a cleared contractor in the NISP, your main duty is to ensure that your facility abides by the terms of the *Security Agreement* DD Form 441 (Department of Defense Security Agreement that is a legal and binding agreement with the government which outlines the terms for safeguarding classified information). This duty involves the oversight of security practices at your facility and cooperation with DSS in maintaining a viable security program. A security program is more than just a matter of physically protecting information. If you work at a non-possessing facility there are still security requirements to be met at your facility. These requirements apply equally to all types of facilities. One of the most important aspects of your job will be to educate all cleared personnel as to their security responsibilities. Throughout the remainder of this course we will explore the details of your job as an FSO, what you have to do and when, as well as, what resources are available to help you.

THE FSO AND THE IS REP

As a Facility Security Officer (FSO), your point of contact with DSS is your ***INDUSTRIAL SECURITY REPRESENTATIVE (IS REP)***. The IS Rep serves as a representative of the U. S. Government in those matters of industrial security covered by the National Industrial Security Program (NISP). The IS Rep does not function as a police officer. Your IS Rep is assigned to work with you in developing and maintaining your security program.



The FSO will most commonly see an IS Rep in one of the following situations:

- During an initial survey when a new facility is being processed for a security clearance;
- When necessary to provide advice and assistance;
- When performing a scheduled security review. These reviews/inspections and surveys are discussed in lesson 9.

STRUCTURE OF DSS: INDUSTRIAL SECURITY

DSS Headquarters is presently located in Alexandria, Virginia. Its mission is accomplished through the efforts of highly skilled personnel assigned to field offices located throughout the United States. Each IS Representative is assigned to a field office.

Each field office is managed by a Field Office Chief (FOC). There is a Deputy Field Director who oversees the operation of all field offices within each of five geographical areas.

The services of a DSS Information Systems Security Professional (ISSP) and a Counterintelligence Specialist (CI) are available to each field office. The DSS Office of Security Services International (OSSI) provides support to cleared contractor employees at overseas locations.

Feel free to visit the DSS website www.dss.mil and click on “**about DSS**” to see more detailed information regarding the organization and location of DSS Offices.

The map shows the areas of responsibility.

DSS INDUSTRIAL SECURITY AREAS OF RESPONSIBILITY

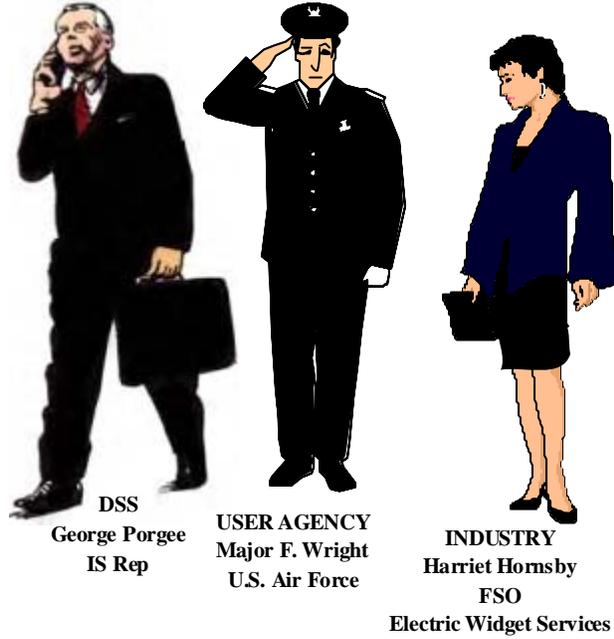


SUMMARY

The NISP is a program to safeguard classified information entrusted to industry. For DoD, there are three components of the NISP: 1) The User Agency, which releases the information; 2) the cleared contractor, who receives or has access to the information; and 3) the Defense Security Service, which oversees the security program of the cleared contractor(s). As an FSO, it is your job to work with DSS in creating and maintaining an adequate security program at your facility based on the guidelines set out by the NISP. The guidelines of the NISP are stated in the National Industrial Security Program Operating Manual (NISPOM). This is a team effort. The protection

of classified information and thereby the maintenance of national security is the ultimate result of this effort.

MEMBERS OF THE GOVERNMENT-INDUSTRY TEAM



1 - REVIEW EXERCISES

Complete the following exercises for review and practice.

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



1. The purpose of the National Industrial Security Program is to
s_____ c_____ i_____ in the hands of i_____.

2. Using the following terms, write a brief definition of "classified information":

- official government information
- protection
- unauthorized Disclosure
- national security
- identified
- TOP SECRET, SECRET, or CONFIDENTIAL.

3. Complete these definitions of the three classification categories:

- a. CONFIDENTIAL: Classified information or material which requires p_____, the unauthorized disclosure of which could reasonably be expected to cause d_____ to the national security that the original classification authority is able to identify or describe.

- b. SECRET: Classified information or material which requires a s_____ d_____ of p_____, the unauthorized disclosure of which could reasonably be expected to cause s_____ d_____ to the national security that the original classification authority is able to identify or describe.

- c. TOP SECRET: Classified information which requires the h_____ d_____ of p_____, the unauthorized disclosure of which could reasonably be expected to cause e_____ g_____ d_____ to the national security that the original classification authority is able to identify or describe.

4. All federal government departments and agencies that classify information are User Agencies within the NISP.

True False

5. Only components of the Department of Defense are User Agencies within the NISP.

True False

6. About half of the cleared contractors within the NISP possess classified information at their own facilities.

True False

7. The four Cognizant Security Agencies that oversee the NISP are:

- a. D_____ of D_____.

- b. D_____ of E_____.

- c. N_____ R_____ C_____.

- d. C_____ I_____ A_____.

8. Match the descriptions with the DoD NISP components.

Component	Description
_____ User Agency	a. provides advice, assistance, and oversight to industry in implementing security requirements.
_____ cleared contractor	b. government customer of private industry.
_____ Defense Security Service	c. provides goods or services that entail access to classified information.
	d. owns classified information generated during performance of classified contract.
	e. requires a Facility Security Clearance to be eligible for access to classified information.

9. A Facility Security Officer's responsibilities include

- () a. educating cleared employees in their security responsibilities.
- () b. ensuring that the facility carries out its obligations under the Security Agreement.
- () c. cooperating with DSS to maintain an adequate security program.
- () d. establishing the requirements for marking and safeguarding classified information possessed by the facility.

10. Match the descriptions with the DSS elements.

DSS Element	Description
_____ IS Rep	a. Official government information which has been determined to require protection against unauthorized disclosure in the interest of National Security and identified as TOP SECRET, SECRET and CONFIDENTIAL. (Pg. 1-3)
_____ NISP	b. Ensures that a cleared facility abides by the terms of the Legal and Binding Security Agreement DD Form 441 which outlines the terms for safeguarding classified information. (Pg. 1-10)
_____ Classified Information	c. an FSO's point of contact with DSS. (Pg. 1-10)
_____ FSO	d. a partnership between the Federal government and private industry to safeguard classified information. (Pg 1-1).
_____ DSS Headquarters	e. located in Alexandria, VA. (Pg. 1-11)

1 – Solutions & References



1. safeguard, classified information, industry. (p. 1-2)
2. Your definition should be about the same as the one given on p. 1-3.
3. a: protection, damage;
b: substantial degree, protection, serious damage;
c: highest degree, protection, exceptionally grave damage.
(pp. 1-4, 5)
4. False. (p. 1-6)
5. False. (p. 1-6)
6. True. (p. 1-7)
7. a. Department of Defense.
b. Department of Energy.
c. Nuclear Regulatory Commission.
d. Central Intelligence Agency. (p. 1-2)
8. b, d User Agency; c, e cleared contractor; a Defense Security Service.
(pp. 1-6--8)
9. a, b, c (p. 1-10)
10. a. Classified Information; b. FSO; c. IS Rep; d. NISP; e. DSS Headquarters.
(pp. 1-1, 1-3, 1-10, 1-11)

LESSON 2

Overview of the National Industrial Security Program Operating Manual (NISPOM)

In 1951 the Munitions Board (now defunct) issued a slim 14-page pamphlet entitled *Industrial Security Manual for Safeguarding Classified Information (ISM)*. Over the years the ISM grew and grew to 400-plus pages. Then in 1995 the ISM was replaced by the *National Industrial Security Program Operating Manual (NISPOM)*, which contains some 130 pages without supplements. As the FSO, a large part of your job is to see that the NISPOM requirements that apply to your facility are implemented.

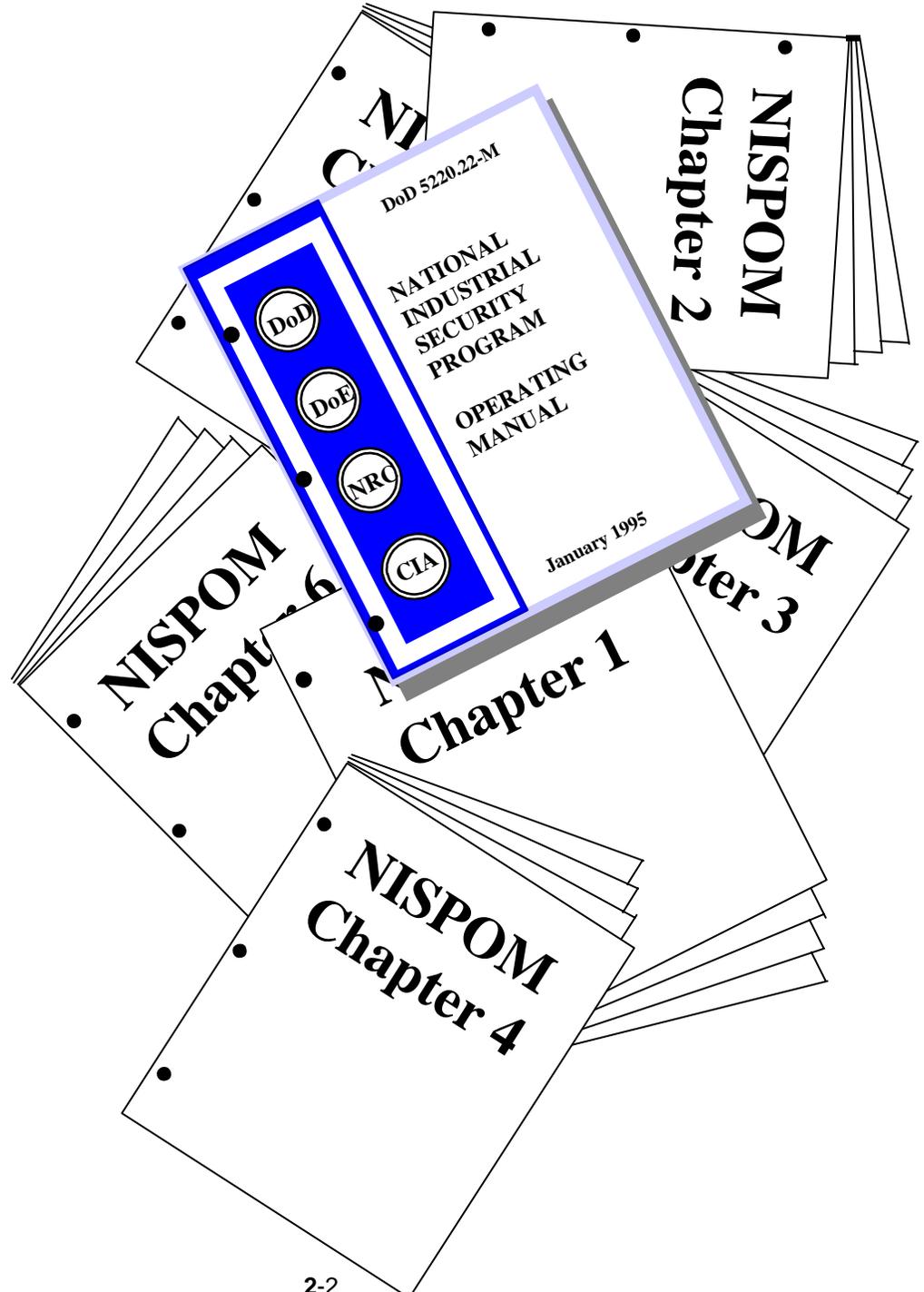
In this lesson we will point out the parts of the NISPOM that apply to *every* facility in the NISP. If your facility does not possess classified material, you may find that only Chapters 1, 2, 3, 6, and appendices A & C will apply.

Note: The other parts of the NISPOM may apply to a non-possessing facility, for instance **Chapter 9, Special Requirements**. To be certain of which chapters apply to your facility, it is recommended that you contact your IS Representative for guidance. We will discuss most of the essential parts of the NISPOM in detail in later lessons. Here, we're just pointing them out to you.

OBJECTIVES

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

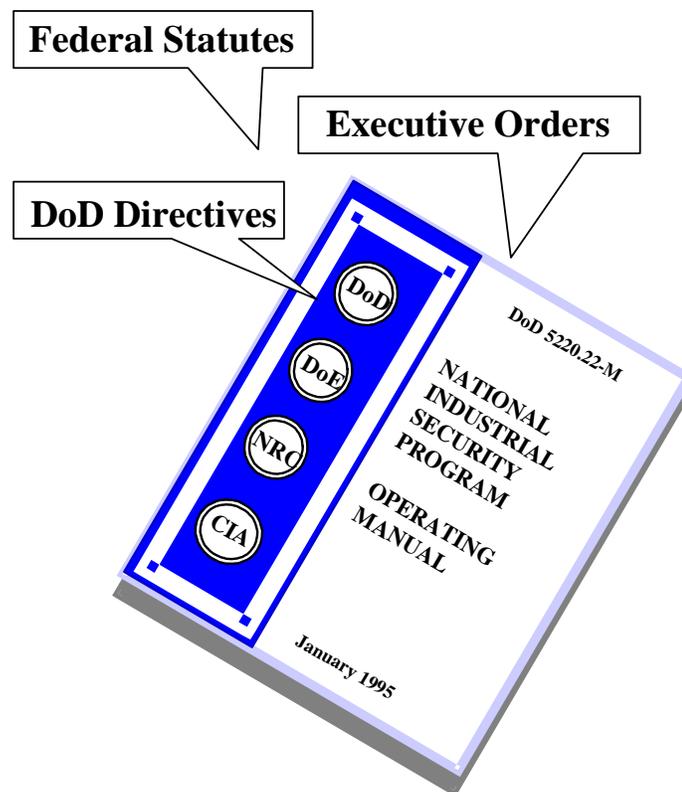
- Describe the format of the NISPOM.
- Identify the parts of the NISPOM that apply to all cleared contractors in the NISP.



IMPORTANCE OF THE NISPOM

The NISPOM is a part of your firm's contract with the government. In signing the Security Agreement (DD Form 441), the management of your facility agreed to comply with the requirements of the NISPOM.

Where did these requirements come from? The NISPOM is a digest or compilation of the various security requirements contained in a wide range of *federal statutes, directives and executive orders*. The NISPOM is your primary reference regarding the protection of classified information.



Familiarizing yourself with the NISPOM is a fundamental way for you to "work smarter." Your firm's management is justifiably concerned with the "bottom line." You can contribute to your firm's profitability by keeping security costs down. One effective way to do this is to be sure that you know which NISPOM security measures apply to your facility and which do not. IS Representatives often discover during facility reviews that some facilities have established security measures not required by the

NISPOM because the FSO mistakenly thought that they were required. *Moral: Know your NISPOM; it's good business.*

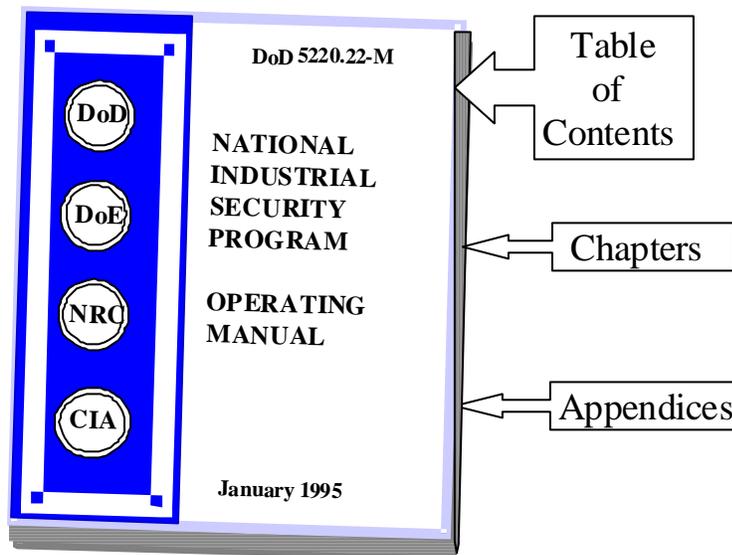
The NISPOM sets forth requirements for implementation by you, the FSO. Security guidance should be provided to company employees by providing them a copy of the Standard Practice and Procedures (SPP) as referenced in Chapter 1-202, NISPOM. The SPP tells your company's employees specifically how your company implements the requirements of the NISP.

INDUSTRIAL SECURITY LETTERS

The Department of Defense-Defense Security Service, publishes an Industrial Security Letter (ISL) periodically to inform Industry, User Agencies and DoD Activities of developments relating to industrial security. ISLs are used to provide detailed operational guidance and to notify you of changes to existing policies or requirements. All ISL's are posted on the DSS Website: www.dss.mil

FORMAT OF THE NISPOM

Let's take a look at the NISPOM. First comes the **TABLE OF CONTENTS**. *Note: The eleven chapters are comprised of sections.*



Each page has a *three-part* number that identifies it by chapter, section, and page:

chapter number - section number - page number

The page number that begins each section is always 1 because the pages of each section are numbered consecutively *within that section* (1-1-1, 1-1-2, 1-1-3).

After the chapters come three **APPENDICES**, lettered A through C. As with the sections, the pages of each appendix are numbered consecutively *within that appendix* (A-1, A-2, A-3).

Last listed are the **SUPPLEMENTS TO THE NISPOM**. The supplements are *separate booklets* and are not included in the main manual, so there are no page numbers for them.

One more thing. The format for subparagraphs is as follows:

1-100.

a.

(1)

(a)

That's about all you need to know to find your way around in the NISPOM. Now let's look at the parts of the manual you will be using the most.

BASIC PARTS OF THE NISPOM

The following NISPOM references apply to *every* contractor in the NISP:

BASIC NISPOM PARTS

CHAPTER 1	GENERAL PROVISIONS AND REQUIREMENTS
CHAPTER 2	SECURITY CLEARANCES
CHAPTER 3	SECURITY TRAINING AND BRIEFINGS
CHAPTER 6	VISITS AND MEETINGS

Appendix A	Organizational Elements for Industrial Security
-------------------	--

Appendix C	Definitions
-------------------	--------------------

As we've indicated, we'll leave the discussions of most of these parts for later lessons. For now, let's look at **Chapter 1**.

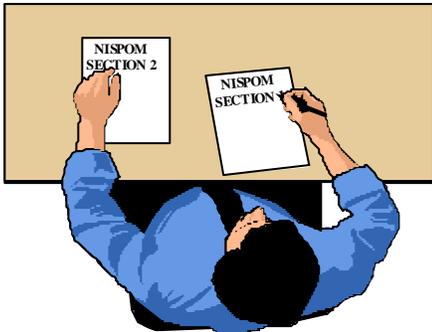
CHAPTER 1 OF THE NISPOM

Chapter 1, General Provisions and Requirements, is the most important part of the NISPOM. It conveys the basic policies of the NISP. The other parts of the NISPOM support Chapter 1.

Now for more good news: of the three sections of Chapter 1, only Section 1 and about half of sections 2 and 3 apply to every contractor in the NISP.

SECTION 1

WAYS TO CUT YOUR NISPOM IN HALF



FOLLOW THE GUIDELINES PROVIDED IN THIS COURSE.

Let's look at Section 1, Introduction. Paragraph 1-100, **Purpose**, states the two main goals of the manual: to *prevent unauthorized disclosure of* and to *control authorized disclosure of* classified information released to NISP contractors. Paragraph 1-101, **Authority**, cites the main executive orders and other sources of authority that underpin the NISP. It points out the role of the Secretary of Defense in administering the NISP, and specifies the roles of the heads of the DOE, NRC, CIA, and the Information Security Oversight Office (ISOO) within the NISP. We have already gone over most of the content of paragraphs 1-102, **Scope**, 1-103, **Agency Agreements**, and 1-104, **Security Cognizance**. Paragraphs 1-105, **Composition of Manual**, 1-106, **Manual Interpretations**, and 1-107, **Waivers and Exceptions to this Manual**, need not concern us here. (Note that in 1-105 "baseline" refers to what applies to every possessing NISP contractor, so it includes all of Chapters 1 through 11. We use "basic" to refer to what in the NISPOM applies to every NISP contractor, whether or not they possess classified material at their facilities.)

SECTION 2

This is a vital section for you to know. **Section 2, General Requirements**, spells out the primary requirements that a cleared contractor is responsible for implementing. *The second requirement in section 2 is the basis for your job.*

1-201. Facility Security Officer (FSO). The contractor shall appoint a U.S. citizen employee, who is required to be cleared as part of the Facility Clearance (FCL), to supervise and direct security measures necessary for implementing this manual and related federal requirements for classified information.

Seven of the ten paragraphs of **Section 2** apply to every cleared contractor in the NISP, as follows. We'll be discussing most of these in later lessons.

BASIC REQUIREMENTS

1-200. General

1-201. Facility Security Officer (FSO)

1-202. Standard Practice Procedures

1-204. Cooperation with Federal Agencies

1-206. Security Training and Briefings

1-207. Security Reviews

1-208. Hotlines

SECTION 3

Section 3. Reporting Requirements, lists the reports contractors are required to submit. The chart shows the reports that every cleared contractor in the NISP must submit, as necessary.

BASIC REPORTS

NISPOM 1-301. Reports to be Submitted the to the FBI:

[Espionage, Sabotage,
or Subversive Activities]

NISPOM 1-302. Reports to be Submitted to (DISCO)

- a. Adverse Information
- b. Suspicious Contacts
- c. Change in Employee's Status
- d. Representative of a Foreign Interest
- e. Citizenship by Naturalization
- f. Employees Desiring Not to Perform on Classified Work
- g. Standard Form (SF) 312

NISPOM 1-304 Individual Culpability Reports

NISPOM 1-302 Reports submitted to DSS Field Office:

- h. Changed Conditions Affecting the Facility Clearance
- m. Employee Information in Compromise Cases

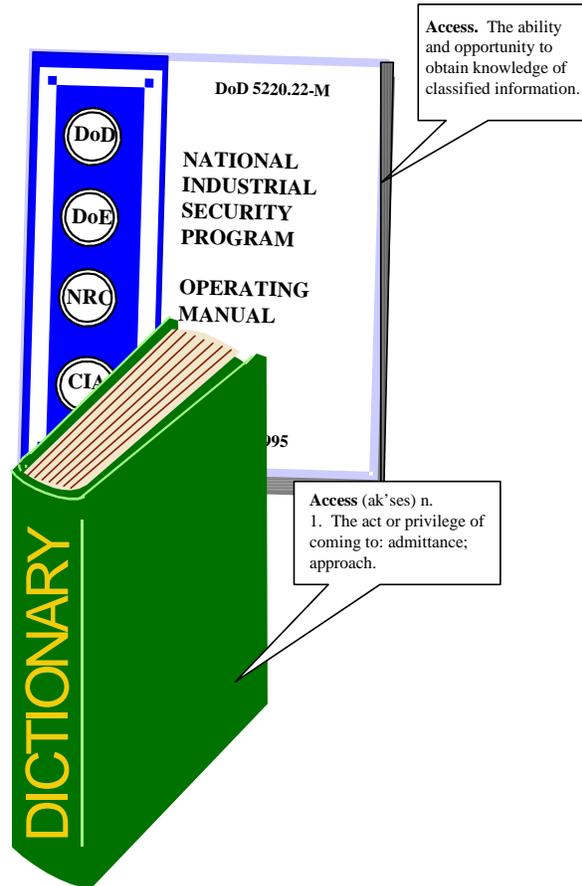
NISPOM 1-303 Reports of Loss, Compromise or Suspected Compromise, and Security Violations

NOTE: In the Industrial Security Letter (ISL) 02L-1, item number 9 (Reports Submitted to the Cognizant Security Agency (CSA) indicates where reports should be sent as referenced in NISPOM Chapters 1-302, 1-303, and 1-304.

APPENDICES

Appendix A, Organizational Elements for Industrial Security, provides a listing of addresses and telephone numbers. In addition to what you find in Appendix A, the Defense Security Service provides a more detailed and updated directory of information online at www.dss.mil.

Now let's turn to **Appendix C, Definitions**. One of the keys to understanding the NISP and to performing your duties within it is to get to know its language. Therefore, in addition to the basic acronyms and abbreviations given at the front of this booklet, you should also learn the meanings of certain basic terms listed in **Appendix C**. You need to learn their meanings because they are often quite different from standard dictionary definitions. Take the definition of "access," for instance. One desk dictionary defines "access" as "the act or privilege of coming to; admittance; approach." Within the NISP, however, "access" means "the ability and opportunity to obtain knowledge of classified information." Quite a difference!



Of the 150 or so terms in **Appendix C**, which ones should you be familiar with? We have listed 32 of them.

KEY TERMS

Access	Home Office Facility
Adverse Information	Industrial Security
Authorized Person	Information
Classified Contract	Limited Access Authorization
Classified Information	Multiple Facility Organization
Cognizant Security Agency	National Security
Cognizant Security Office	Need-to-Know
Compromise	Parent Corporation
CONFIDENTIAL	Personnel Security Clearance
Contractor	Public Disclosure
Document	Representative of a Foreign Interest
Facility	SECRET
Facility Security Clearance	Security Cognizance
Foreign Interest	Subsidiary Corporation
Foreign Nationals	TOP SECRET
Government Contracting Activity	Unauthorized Person

SUMMARY

The NISPOM is a synthesis of various federal security requirements. The NISPOM is a part of your firm's contract with the government, and your most important duty as an FSO is to ensure that your company complies with applicable provisions of the NISPOM. Only a few parts of the NISPOM apply to every cleared contractor in the NISP. In general, the parts discussed in this lesson are the only ones that a non-possessing facility needs to concern itself with.

2 - Review Exercises

Complete the following exercises for review and practice.

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



1. The management of your firm has formally agreed with the government to comply with the provisions of the NISPOM.

() True. () False.

2. The provisions of the NISPOM are derived from security requirements established by federal statutes, executive orders, and federal directives.

() True. () False.

3. The two main goals of the NISPOM are 1) to p_____ u_____ disclosure and 2) to c_____ a_____ disclosure of classified information released by elements of the executive branch to their contractors.

4. The Table of Contents lists

() a. Chapters.

() b. Sections.

() c. Paragraphs.

() d. Appendices.

() e. Supplements.

() f. Figures.

5. 5-3-2 refers to _____ of _____ of _____ of the NISPOM.

6. The COMSEC Supplement is included at the rear of the manual.

() True. () False.

7. The tenth paragraph of Section 3 of Chapter 2 is numbered

() a. 3-209.

() b. 2-310.

() c. 9-203.

8. Only about four chapters and two appendices of the NISPOM generally apply to every contractor in the NISP.

() True. () False.

9. The other parts of the NISPOM support and supplement

() a. Chapter 1, General Provisions and Requirements.

() b. Chapter 2, Security Clearances.

() c. Chapter 3, Security Training and Briefings.

() d. Chapter 6, Visits and Meetings.

10. Match the following sections of NISPOM, Chapter 1, with their topics.

Section	Topic
_____ Section 1.	a. Reporting Requirements
_____ Section 2.	b. Introduction
_____ Section 3.	c. General Requirements

2 - Solutions & References



1. **True.** (p. 2-3)
2. **True.** (p. 2-3)
3. prevent unauthorized, control authorized. (p. 2-6)
4. a., b., d., and e. (p. 2-4)
5. chapter, section, page (p. 2-5)
6. **False.** (p. 2-5)
7. b. (p. 2-5)
8. **True.** (p. 2-5)
9. a. (p. 2-5)
10. b. Section 1.
c. Section 2.
a. Section 3. (pp. 2-5-6--7)

LESSON 3

The Facility Security Clearance

So far we've given you general overviews of the NISP and the NISPOM. Beginning with this lesson we'll be discussing the specifics of your duties as an FSO. In this lesson we'll be talking about what a facility is, why the NISP requires its facilities to be cleared, and what is involved in granting a facility security clearance (FCL). You need to know these things so that you will know what conditions and factors bear directly on your FCL. Then, when changes occur, you will be able to take the correct action to ensure that your facility maintains its clearance or, if appropriate, terminates its clearance on good terms with the NISP. In this lesson we will discuss many of these "changed conditions" and how you should handle them.

OBJECTIVES

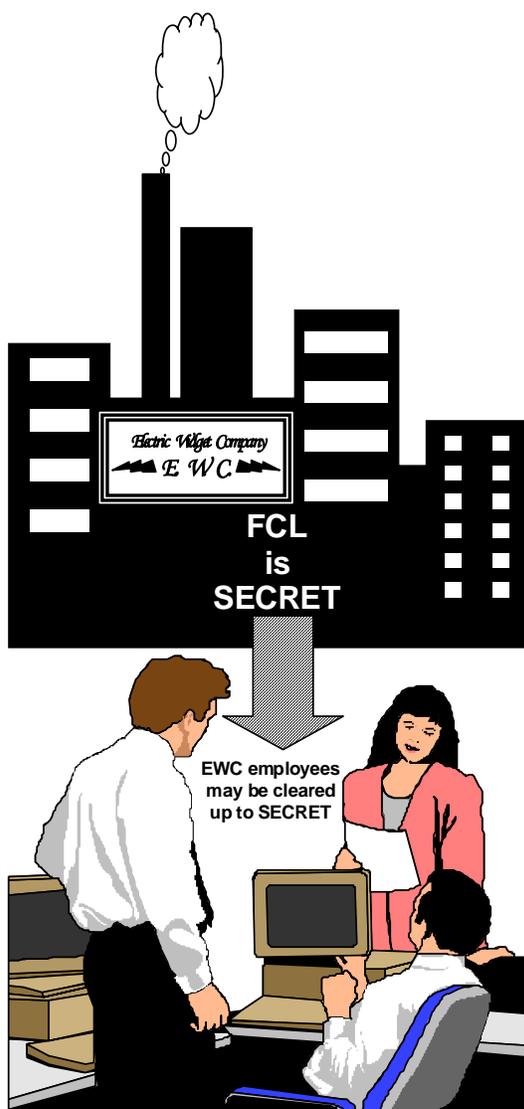
When you have completed this lesson, you should be able to do the following:

- Explain briefly what a facility is within the NISP.
- Explain briefly what a facility security clearance (FCL) is, its purpose, and what considerations it is based on.
- Identify changed conditions that require action by the FSO and what actions are appropriate in each case.

FACILITY

For the purposes of the NISP, a facility must be organized and existing under the laws of any of the 50 states, District of Columbia (D.C.) or Puerto Rico, and be located in the U.S. or its territorial areas or possessions. A facility must have a demonstrated reputation for integrity and lawful conduct in business dealings and must not be under foreign ownership, control or influence (FOCI) to such a degree that the granting of a clearance may place classified information in danger of inadvertent or unauthorized disclosure. You'll find the official NISP definition of "facility" in **Appendix C** of the NISPOM. For our purposes, a working definition should do. Quite simply, a facility is either (1) *the site/premises of a contractor (company)*, or (2) *a geographically separate operating location of the contractor (e.g., in another city or state)*.

FACILITY SECURITY CLEARANCE



A Facility Security Clearance is "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)," (**Appendix C, NISPOM**). The administrative determination is made by the Defense Industrial Security Clearance Office (DISCO). Note: That a FCL is not a blanket authorization for all contractor employees to have access to classified information. It merely states the highest category of classified information to which personnel at that facility, when they have been individually cleared at that level, may be authorized access to classified material.

PURPOSE OF A FACILITY SECURITY CLEARANCE

A facility security clearance is a broad-based determination that addresses the realities of private industry as it is structured and operates in the United States. It is a means of making security work within the profit-oriented, "hardball" arena of competitive private enterprise. This determination takes into account that:

- There are a variety of business structures in the U.S., ranging from the small sole proprietorship to the giant corporation;
- The "legal entities" of these business structures differ from one structure to another as accountable parties in the eyes of the law, such as:
 - A facility can be controlled by another facility;
 - A business operating in the US can be owned, controlled, or influenced by foreign interests;
 - The managers of a facility, and those who influence them, directly affect its operation; and
 - All of these considerations bear on the fitness of a facility (and its employees) to be granted access to classified information.

We can summarize these considerations by stating that clearing a facility mainly entails; 1) identifying and assessing, from a security standpoint, the sources of power, both domestic and foreign, that affect that facility; and 2) where these are found to be acceptable, binding the facility's management, via the Security Agreement, to carry out the provisions of the NISPOM.

The evaluation is conducted and the Security Agreement is executed to ensure that *no source of power will be permitted to adversely affect the protection of classified information or material to which the facility has access.*

THE FIVE ESSENTIAL ELEMENTS

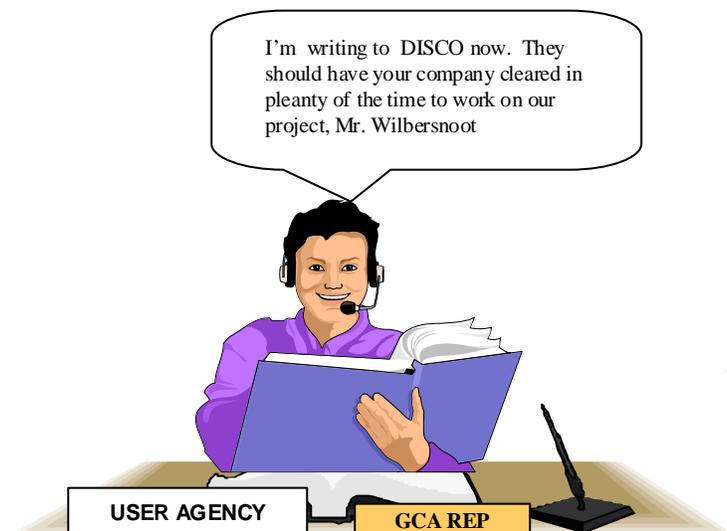
Let's examine what's involved for your facility to be granted a clearance. DISCO bases its determination on the following considerations, which are referred to as "five essential elements:"

5 ELEMENTS

1. Sponsorship
2. Security Agreement
3. Certificate Pertaining to Foreign Interests
4. Organization
5. Key Management Personnel Clearances

Your facility has to satisfy the above requirements in all five areas to be issued a facility clearance.

SPONSORSHIP



Facility clearance actions begin when the U.S. Government contracting activity (GCA) of a User Agency (UA) decides to issue a classified contract. A classified contract is "any contract that requires or will require access to classified information by the contractor or his or her employees in the performance of the contract" (**Appendix C, NISPOM**). Note: While contractors have to be cleared to perform under classified contracts, the rules of the NISP state that contractors cannot themselves request that they be cleared. Only a GCA or a currently cleared contractor can request that a facility be processed for an FCL. This request is referred to as sponsorship.

The usual course of sponsorship is as follows: The GCA identifies prime contractors who will require access to classified information to 1) prepare their bids or proposals for the classified contract, and/or 2) perform under the classified contract when it is awarded. These prime contractors identify subcontractors who will require access to classified information for pre-contract activities and/or contract performance.

Specifically, your sponsor requested DISCO to initiate a facility clearance action. The letter identified your facility, described the classified acquisition that required the clearance action, and stated the level of clearance appropriate for your facility. If your facility would be generating and/or receiving classified information, the request also identified appropriate safeguarding requirements.

SECURITY AGREEMENT



**George Porgee
IS REP**

When DISCO received the request from your sponsor, a representative called your facility by phone to gather certain facts essential to start the clearance process. Next, DISCO provided several forms for your management to execute and to give to an IS Rep during the first on-site visit to your facility. One of the most important forms was a *Security Agreement (DD Form 441)*.

Your firm's copy of the agreement should be on file at your facility. A sample DD Form 441 is shown on the following page, so that you may refer to it as we discuss it. In addition, a sample copy of DD Form 441-1 (Appendage to the Security Agreement) that is used to represent divisions or branches of multiple facility organizations under one "Department of Defense Security Agreement" (Attachment to DD Form 441)

The Security Agreement is a legally binding contract between the U.S. Government and the contractor. As such, it is equally binding on both parties. Since there are only six sections to the agreement, we'll discuss them all briefly.

DEPARTMENT OF DEFENSE
SECURITY AGREEMENT

Form Approved
OMB No. 0704-0194
Expires Jun 30, 2004

The public reporting burden for this collection of information is estimated to average 14 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0194), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS. RETURN COMPLETED FORM TO YOUR RESPECTIVE COGNIZANT SECURITY OFFICE.

This DEPARTMENT OF DEFENSE SECURITY AGREEMENT (hereinafter called the Agreement) , entered into this _____ day of _____, _____ by and between THE UNITED STATES OF AMERICA through the Defense Security Service

acting for the Department of Defense and other governmental User Agencies (hereinafter called the Government) , and

_____ (hereinafter called the Contractor) , which is:

(1) a corporation organized and existing under the laws of the state of _____

(2) a partnership consisting of _____

(3) an individual trading as _____

with its principal office and place of business at (Street, City, State and ZIP Code) _____

WITNESSETH THAT:

WHEREAS, the Government has in the past purchased or may in the future purchase from the Contractor supplies or services, which are required and necessary to the national security of the United States; or may invite bids or request quotations on proposed contracts for the purchase of supplies or services, which are required and necessary to the national security of the United States; and

WHEREAS, it is essential that certain security measures be taken by the Contractor prior to and after being accorded access to classified information; and

WHEREAS, the parties desire to define and set forth the precautions and specific safeguards to be taken by the Contractor and the Government in order to preserve and maintain the security of the United States through the prevention of improper disclosure of classified information, sabotage, or any other acts detrimental to the security of the United States;

NOW, THEREFORE, in consideration of the foregoing and of the mutual promises herein contained, the parties hereto agree as follows.

Section I - SECURITY CONTROLS

(A) The Contractor agrees to provide and maintain a system of security controls within the organization in accordance with the requirements of the "National Industrial Security Program Operating Manual," DoD 5220.22-M (hereinafter called the Manual) attached hereto and made a part of this agreement, subject, however, (i) to any revisions of the Manual required by the demands of national security as determined by the Government, notice of which shall be furnished to the Contractor, and (ii) to mutual agreements entered into by the parties in order to adapt the Manual to the Contractor's business and necessary procedures thereunder. In order to place in effect such security controls, the Contractor further agrees to prepare Standard Practice Procedures for internal use, such procedures to be consistent with the Manual. In the event of any inconsistency between the Manual, as revised, and the Contractor's Standard Practice Procedures, the Manual shall control.

(B) The Government agrees that it shall indicate when necessary, 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, and the Government shall give written notice of such security classification to the Contractor and of any subsequent changes thereof; provided, however, that matters requiring security classification will be assigned the least restricted security classification consistent with proper safeguarding of the matter concerned, since overclassification causes unnecessary operational delays and depreciates the importance of correctly classified matter. Further, the Government agrees that when Atomic Energy information is involved it will, when necessary, indicate by a marking additional to the classification marking that the information is "RESTRICTED DATA." The "Department of Defense Contract Security Classification Specification" (DD Form 254) is the basic document by which classification, regrading, and declassification specifications are documented and conveyed to the Contractor.

(C) The Government agrees, on written application, to grant personnel security clearances to eligible employees of the Contractor who require access to information classified TOP SECRET, SECRET, or CONFIDENTIAL.

(D) The Contractor agrees to determine that any subcontractor, subbidder, individual, or organization proposed for the furnishing of supplies or services which will involve access to classified information, has been granted an appropriate facility security clearance, which is still in effect prior to according access to such classified information.

Section II - SECURITY REVIEWS

Designated representatives of the Government responsible for reviews pertaining to industrial plant security shall have the right to review, at reasonable intervals, the procedures, methods, and facilities utilized by the Contractor in complying with the requirements of the terms and conditions of the Manual. Should the Government, through its authorized representative, determine that the Contractor's security methods, procedures, or facilities do not comply with such requirements, it shall submit a written report to the Contractor advising of the deficiencies.

Section III - MODIFICATION

Modification of this Agreement may be made only by written agreement of the parties hereto. The Manual may be modified in accordance with Section I of this Agreement.

Section IV - TERMINATION

This Agreement shall remain in effect until terminated through the giving of 30 days' written notice to the other party of intention to terminate; provided, however, notwithstanding any such termination, the terms and conditions of this Agreement shall continue in effect so long as the Contractor possesses classified information.

Section V - PRIOR SECURITY AGREEMENTS

As of the date hereof, this Agreement replaces and succeeds

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the day and year written above: THE

any and all prior security or secrecy agreements, understandings, and representations, with respect to the subject matter included herein, entered into between the Contractor and the Government; provided, that the term "security or secrecy agreements, understandings, and representations: shall not include agreements, understandings, and representations contained in contracts for the furnishing of supplies or services to the Government which were previously entered into between the Contractor and the Government.

Section VI - SECURITY COSTS

This Agreement does not obligate Government funds, and the Government shall not be liable for any costs or claims of the Contractor arising out of this Agreement or instructions issued hereunder. It is recognized, however, that the parties may provide in other written contracts for security costs, which may be properly chargeable thereto.

UNITED STATES OF AMERICA

By _____
(Signature of Authorized Government Representative)

(Typed Name of Authorized Government Representative)

(Typed Name of Authorized Government Agency)

(Typed Name of Contractor Entering Agreement)

WITNESS

By _____
(Signature of Authorized Contractor Representative)

(Typed Name of Authorized Contractor Representative)

NOTE: In case of a corporation, a witness is not required but the certificate must be completed. Type or print names under all signatures.

(Title of Authorized Contractor Representative)

(Contractor Address)

(Contractor Address)

NOTE: Contractor, if a corporation, should cause the following certificate to be executed under its corporate seal, provided that the same officer shall not execute both the Agreement and the Certificate.

CERTIFICATE

I, _____, certify that I am the _____
of the corporation named as Contractor herein; that _____
who signed this Agreement on behalf of the Contractor, was then _____
of said corporation; that said Agreement was duly signed for and in behalf of said corporation by authority of its governing body, and is
within the scope of its corporate powers.

(Corporate Seal)

(Signature and Date)

APPENDAGE TO DEPARTMENT OF DEFENSE SECURITY AGREEMENT

Form Approved
OMB No. 0704-0194
Expires Jun 30, 2004

The public reporting burden for this collection of information is estimated to average 10 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0194), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS. RETURN COMPLETED FORM TO YOUR RESPECTIVE COGNIZANT SECURITY OFFICE.

It is further agreed, on this _____ day of _____ by and between the United States of America through the Defense Security Service, acting for the Department of Defense, hereinafter called the Government, and _____ which has entered into the Security Agreement to which this appendix is made a part that the branches and/or facilities listed below, owned and/or operated by said contractor are included in and covered by the provisions of the said Security Agreement, and Certificate Pertaining to Foreign Interests, Standard Form 328.

NAME OF PLANT OR FACILITY	NUMBER AND STREET ADDRESS	CITY AND STATE

THE UNITED STATES OF AMERICA	CONTRACTOR <i>(Typed Name)</i>
BY <i>(Signature of Government Representative)</i>	BY <i>(Signature of Authorized Contractor Representative)</i>
AUTHORIZED REPRESENTATIVE OF THE GOVERNMENT <i>(Typed Name of Government Agency)</i>	TITLE <i>(of Authorized Contractor Representative)</i>
	ADDRESS

Section I - SECURITY CONTROLS. Under this section your firm agreed to do four things.

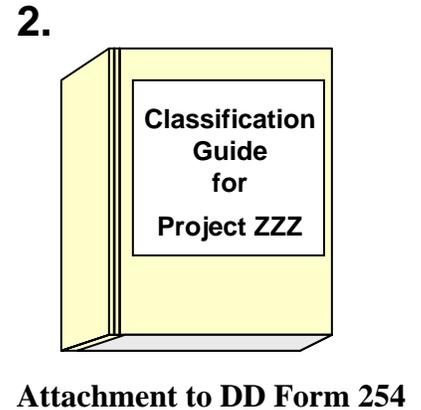
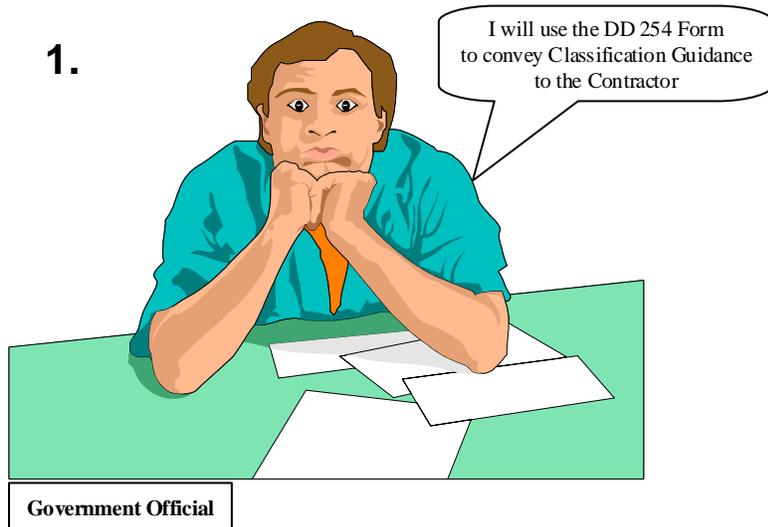
1. **Provide and maintain a system of security controls within the organization in accordance with NISPOM requirements.** This means that it is mainly up to the contractor and to you as the FSO to implement and monitor security measures at your facility. Note that the NISPOM becomes part of the Security Agreement.

2. **Prepare Standard Practice Procedures (SPP) that are consistent with the NISPOM.** Every facility must have procedures for internal use, consistent with the NISPOM.

The NISPOM does not require the SPP to be in written form in every case, however each facility must have standard procedures for implementation of the NISPOM provisions.

3. **Comply with revisions to the NISPOM.** Your facility should implement a revision immediately.

4. **Determine that any "subcontractor, sub-bidder, individual, or organization" that will require access to classified information has a valid FCL at the proper level.** Usually you determine this by contacting the Defense Security Service - Central Verification Activity (DSS-CVA).



Under Section I the U.S. Government agrees to do two things:

1. **Provide classification guidance to the contractor regarding both U.S. Government-furnished and contractor-generated "supplies, services, and other matters."** The U.S. Government provides this guidance primarily through an attachment to every classified contract: the DD Form 254, "The Contract Security Classification Specification." The DD Form 254 tells the contractor what needs to be protected and to what level. Note that most classified contracts, i.e., the agreement documents, are not themselves classified. Also that the U.S. Government will assign the least restrictive classification possible to classified information. Contractors are required to discuss the classification guidance with the GCA whenever the contractor thinks that the guidance is improper or inadequate. (See 4-104, NISPOM.)

2. **Process the contractor's employees for appropriate clearances as required.** We'll talk about personnel security clearances in the next lesson.

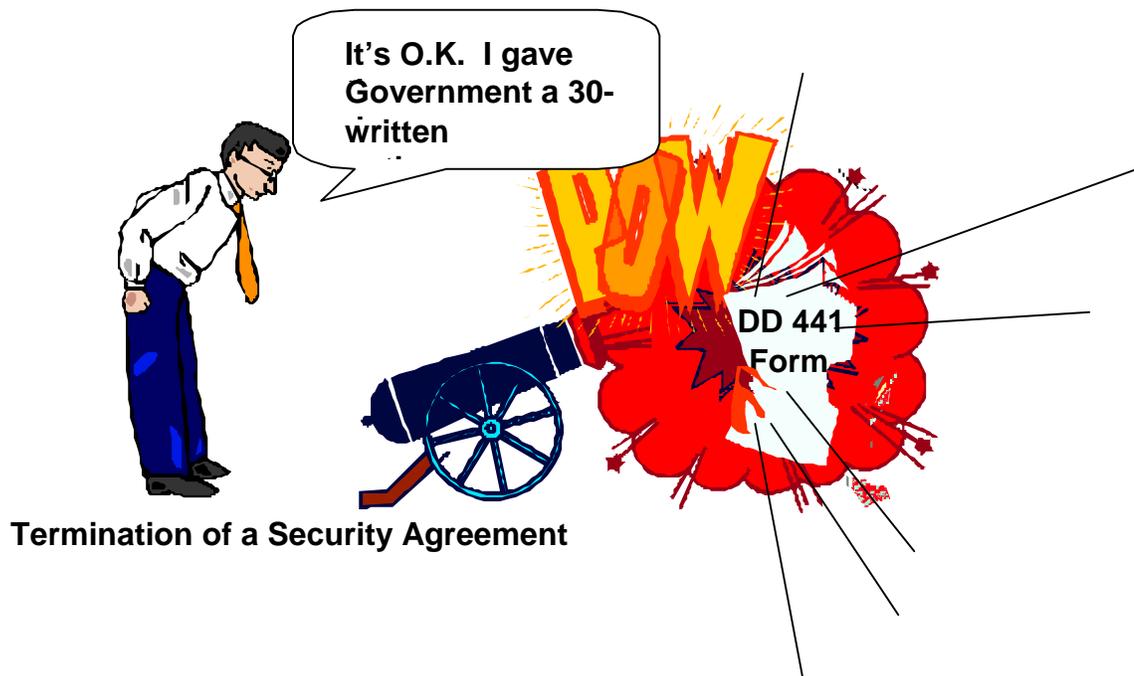


PCL PROCESSOR Model 4823 Patent Pending

Section II – SECURITY REVIEWS: This two-sentence section may be the one of most interest to you. Here, the U.S. Government establishes its right to review, at reasonable intervals, the procedures, methods, and facilities that you use to comply with NISPOM requirements. (Just what is a "reasonable interval" depends, in part, on whether your facility possesses classified information. Currently, a "reasonable interval" may be once per year.) Remember the DSS inspections may either be announced beforehand or unannounced. This section also requires DSS's IS Reps to provide your company a written report of any significant deficiencies they find. The purpose of these reports are to inform your facility of the nature of the discrepancy and then to explain what corrective action is needed for your facility to achieve compliance with NISPOM requirements. We'll discuss reviews in Lesson 9.

Section III - MODIFICATION. As with most contracts, the Security Agreement does provide for modification in exceptional circumstances. However, this is seldom, if ever, done. Remember, under Section I, the NISPOM can be and is modified (revised) unilaterally by the U.S. Government.

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, your facility's personnel are obligated to protect any classified information still in their possession or under their control *as if the agreement had not been terminated.* (This includes classified information "in their heads.")



Section V - PRIOR SECURITY AGREEMENTS. This section simply establishes that, except for security provisions in existing contracts between the U.S. Government and the contractor, this agreement is now the one that counts regarding its subject matter (security controls, security reviews, etc.).

Section VI - SECURITY COSTS. This section means that *this* agreement does *not* obligate the U.S. Government to pay for the contractor's costs in establishing security controls (buying security containers, constructing controlled areas, taking the time needed to process persons for clearances, etc.). It basically means that security costs should be included in the contractor's bid or proposal along with the contractor's other costs to provide goods and services to the U.S. Government.

CHANGED CONDITIONS: SECURITY AGREEMENT

Certain changed conditions affect your Security Agreement and thus the status of your FCL. You should write a letter (report) to your DSS Field Office as soon as you are aware of any of the following: (1-302h, NISPOM)

1. Change of ownership or stock transfers that affect control of the company.
2. **Change of Operating Name or Address.** Since these are stated in the Security Agreement, changes require that it be re-executed. Changes should be promptly reported.
3. Changes related to Key Management Personnel.
4. **Business Termination.** If your firm is going out of business for any reason or if it becomes involved in bankruptcy action, report the facts to your DSS Field Office immediately.
5. Any change related to foreign ownership, control or influence (FOCI).

3a - Review Exercises

Complete the following exercises for review and practice.

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



1. As a working definition, a facility is either (1) the s_____ /p_____ of a contractor, or (2) a g_____ s_____ location of the contractor.

2. A facility security clearance is an administrative d_____ that, from a security viewpoint, a facility is e_____ for a_____ to classified information of a certain c_____ (and all lower c_____).

3. When a facility clearance is granted, an evaluation is conducted and the Security Agreement is executed to ensure that no source of power will be permitted to adversely affect the protection of classified information or material to which the facility has access.

() True. () False.

4. Facility security clearances are issued by

() a. the Director, DSS.

() b. the Secretary of Defense.

() c. the Director of the CIA.

() d. DISCO.

5. A classified contract is any contract that requires or will require a _____ to c _____ i _____ by the contractor or his or her e _____ in the performance the contract.

6. Uncleared contractors can request that their facilities be processed for facility security clearances.

True. False.

7. Only an U.S. Government Contracting Activity or a cleared contractor can request that a facility be processed for a facility security clearance.

True. False.

8. The Security Agreement (DD Form 441) is a legally binding contract between the U.S. Government and the contractor.

True. False.

9. The U.S. Government provides classification guidance to the contractor mainly through a DD Form _____, "The Department of Defense Contract Security Classification Specification."

15. If your company changes its operating name or address, or if it is going out of business or becomes involved in a bankruptcy action, you must report the change to
- () a. DISCO.
 - () b. Your DSS Field Office.
 - () c. DSS Headquarters.
 - () d. The Secretary of Defense.
16. DD Form 441-1, is a legally binding contract between the U.S. Government and the contractor that represents divisions or branches of multiple facility organization under one Department of Defense Security Agreement.
- () True
 - () False

Have any of these changes occurred at your facility? Are any anticipated?

<p>Change of Organizational Name or Address</p>	<p>Business Termination</p>		
<p>Key Management becomes a Representative of a Foreign Interest.</p>	<p>Change (Gain or Loss) of Key Management Personnel</p>	<p>Change in Organizational Structure</p>	<p>Change in Foreign Ownership, Control or Influence</p>

3a - Solutions & References



1. site/premises; geographically separate. (p. 3-2).
2. determination, eligible, access, category, categories. (p. 3-2).
3. True. (p. 3-3).
4. d. (p. 3-4).
5. access, classified information, employees. (p. 3-4).
6. False. (p. 3-4).
7. True. (p. 3-4).
8. True. (p. 3-5).
9. 254. (p. 3-10).
10. a., b., c., d (p. 3-10).
11. False. (p. 3-11).
12. 30. (p. 3-12).
13. False. (p. 3-12).
14. False. (p. 3-13).

15. b. (p. 3-13).

16. True (p. 3-5)

CERTIFICATE PERTAINING TO FOREIGN INTERESTS

At about the same time that your facility executed the Security Agreement, it also executed the *Certificate Pertaining to Foreign Interests (Standard Form [SF] 328)*. Instructions for completing the SF 328 are on the next page, and a sample SF 328 is on the pages following. 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 we must determine if these sources of power are foreign interests or influenced by foreign interests. The general policy is that a facility that is determined to be under *foreign ownership, control, or influence (FOCI)* is ineligible for a Facility Security Clearance unless the foreign source can be effectively excluded from any control over classified operations. See **Chapter 2, Section 3, NISPOM**, for additional information.

When is a facility determined to be under FOCI? The all-inclusive, loophole-closing official statement is in **NISPOM, 2-302**. If the DSS Field Office (in coordination with HQ, DSS) after reviewing and analyzing the information furnished by the contractor on the SF 328 finds that "a foreign interest has the power" to affect the facility in a way that may lead to "unauthorized access to classified information or may affect adversely the performance of classified contracts," then the facility is determined to be under FOCI.

If there were any FOCI factors at your facility, either they were not significant enough to disqualify your facility or they have been effectively mitigated.

INSTRUCTIONS FOR COMPLETING THE SF FORM 328.

In completing the SF Form 328, all items are to be answered by indicating X in either the YES or NO column. If an answer to any question is YES, the following paragraphs provide instructions for the submission of the necessary data.

QUESTION 1a: Identify the percentage of any class of stock or other securities issued which are owned by foreign persons, broken down by country. Include indirect ownership through one or more intermediate level(s) of subsidiaries. Indicate voting rights of each class of stock. If there are shareholder agreements attach a copy(ies), and if none, so state. Indicate whether a copy of SEC Schedule 13D/13G report has been received from any investor. If yes, attach a copy(ies). Ownership of less than 5% should be included if the holder is entitled to control the appointment and tenure of any management position.

1b: Identify the percentage of total capital commitment, which is subscribed by foreign persons. If there is an agreement(s) with the subscriber(s), attach a copy(ies), and if none, so state.

QUESTION 2: Identify the foreign interest by name, country, percentage owned and personnel who occupy management positions with the organizations. If there are personnel from your organization who occupy management positions with the foreign firm(s), identify the name(s), title, and extent of involvement in the operations of the organizations (to include access to classified information).

QUESTION 3: Identify the foreign person(s) by name, title, citizenship, immigration status and clearance or exclusion status. Attach copies of applicable by-laws or articles of incorporation, which describe the affected position(s). However, if you have already provided such copies to the Cognizant Security Agency Industrial Security Representative, so state.

QUESTION 4: Identify the foreign person(s) by name, title, citizenship and all details concerning the control or influence. If any foreign person(s) have such power this question shall be answered in the affirmative even if such power had not been exercised and whether or not it is exercisable through ownership of your facility's securities, if such power may be invoked by contractual arrangements or by other means.

QUESTION 5: For each instance, provide the name of the foreign person, country, percentage of gross income derived and nature of involvement including: whether defense/nuclear related or not; involvement with classified or export controlled technology; compliance with export control requirements. Where the organization has a large number of involvements; are not defense/nuclear related and represent a small percentage of gross income, the explanation can be a generalized statement addressing the totals by country.

QUESTION 6: Provide overall debt-to-debt equity ratio (in percentage). With respect to indebtedness or liability to a foreign person, indicate to whom indebted or liable, what collateral has been furnished or pledged and any conditions or covenants of the loan agreement. If stock or assets have been furnished or pledged as collateral, provide a copy of the loan agreement or pertinent extracts thereof (to include procedures to be followed in the event of default). If any debentures are convertible, provide specifics. If loan payments are in default, provide details. Answer in the affirmative if the debt is with a U.S. entity that is owned or controlled either directly or indirectly by a foreign person, if unknown, so state.

QUESTION 7: If YES to either part of the question provide overall percentage of income derived from foreign sources by country, nature of involvement and type of services or products. Indicate if any single foreign source represents in excess of 5% of total revenue or net income. Indicate whether any classified information is involved. State whether facility is in compliance with applicable export control requirements.

QUESTION 8: Identify each foreign institutional investor holding 10% or more of the voting stock by name and address and the percentage of stock held. Indicate whether any investor has attempted to or has exerted any control or influence over appointments to management positions or influenced the policies of the organization. Include copies of SEC Schedule 13D/13G.

QUESTION 9: Provide the name, title, citizenship, immigration status and clearance or exclusion status on all such persons. Identify by name and address each foreign organization with which such persons serve and indicate the capacity in which they are serving. Include a Statement of Full Disclosure of Foreign Affiliations for every cleared individual who is a representative of a foreign interest.

QUESTION 10: Describe the foreign involvement in detail, including why the involvement would not be reportable in the preceding questions.

CERTIFICATE PERTAINING TO FOREIGN INTERESTS <i>(Type or print all answers)</i>		<i>Form Approved OMB No. 0704-0194 Expires Dec 31, 2000</i>	
<p>The public reporting burden for this collection of information is estimated to average 70 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0194), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p>			
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS. RETURN COMPLETED FORM TO YOUR RESPECTIVE COGNIZANT SECURITY OFFICE.			
PENALTY NOTICE			
<p>Failure to answer all questions or any misrepresentation (by omission or concealment, or by misleading, false or partial answers) may serve as a basis for denial of clearance for access to classified information. In addition, Title 18, United States Code 1001, makes it a criminal offense, punishable by a maximum of five (5) years imprisonment, \$15,000 fine or both, knowingly to make a false statement or repre-</p>		<p>sentation to any Department or Agency of the United States, as to any matter within the jurisdiction of any Department or Agency of the United States. This includes any statement made herein which is knowingly incorrect, incomplete or misleading in any important particular.</p>	
PROVISIONS			
<p>1. This report is authorized by the Secretary of Defense, as Executive Agent for the National Industrial Security Program, pursuant to Executive Order 12829. While you are not required to respond, your eligibility for a facility security clearance cannot be determined if you do not complete this form. The retention of a facility security clearance is contingent upon your compliance with the requirements of DoD 5220.22-M for submission of a revised form as appropriate.</p>		<p>2. When this report is submitted in confidence and is so marked, applicable exemptions to the Freedom of Information Act will be invoked to withhold it from public disclosure.</p> <p>3. Complete all questions on this form. Mark "Yes" or "No" for each question. If your answer is "Yes" furnish in full the complete information under "Remarks."</p>	
QUESTIONS AND ANSWERS			
<p>1. <i>(Answer 1a. or 1b.)</i> a. <i>(For entities which issue stock):</i> Do any foreign person(s), directly or indirectly, own or have beneficial ownership of 5 percent or more of the outstanding shares of any class of your organization's equity securities?</p>		YES	NO
<p>b. <i>(For entities which do not issue stock):</i> Has any foreign person directly or indirectly subscribed 5 percent or more of your organization's total capital commitment?</p>			
<p>. Does your organization directly, or indirectly through your subsidiaries and/or affiliates, own 10 percent or more of any foreign interest?</p>			
<p>3. Do any non-U.S. citizens serve as members of your organization's board of directors (or similar governing body), officers, executive personnel, general partners, regents, trustees or senior management officials?</p>			
<p>4. Does any foreign person(s) have the power, direct or indirect, to control the election, appointment, or tenure of members of your organization's board of directors (or similar governing body) or other management positions of your organization, or have the power to control or cause the direction of other decisions or activities of your organization?</p>			
<p>5. Does your organization have any contracts, agreements, understandings, or arrangements with a foreign person(s)?</p>			
<p>6. Does your organization, whether as borrower, surety, guarantor or otherwise have any indebtedness, liabilities or obligations to a foreign person(s)?</p>			
<p>7. During your last fiscal year, did your organization derive: a. 5 percent or more of its total revenues or net income from any single foreign person?</p>			
<p>b. In the aggregate 30 percent or more of its revenues or net income from foreign persons?</p>			
<p>8. Is 10 percent or more of any class of your organization's voting securities held in "nominee" shares, in "street names" or in some other method which does not identify the beneficial owner?</p>			
<p>9. Do any of the members of your organization's board of directors (or similar governing body), officers, executive personnel, general partners, regents, trustees or senior management officials hold any positions with, or serve as consultants for, any foreign person(s)?</p>			
<p>10. Is there any other factor(s) that indicates or demonstrates a capability on the part of foreign persons to control or influence the operations or management of your organization?</p>			
STANDARD FORM 328 (4/1997) (EG)		REPLACES DD FORM 441S, WHICH IS OBSOLETE.	
		Designed using Perform Pro, WHS/DIOR, Jan 98	

REMARKS (Attach additional sheets, if necessary, for a full detailed statement.)

CERTIFICATION

I CERTIFY that the entries made by me above are true, complete, and correct to the best of my knowledge and belief and are made in good faith.

WITNESSES:

_____ (Date Certified)
By _____
_____ (Contractor)

NOTE: In case of a corporation, a witness is not required but the certificate below must be completed. Type or print names under all signatures.

_____ (Title)
_____ (Address)

NOTE: Contractor, if a corporation, should cause the following certificate to be executed under its corporate seal, provided that the same officer shall not execute both the Agreement and the Certificate.

CERTIFICATE

I, _____, certify that I am the _____
of the corporation named as Contractor herein; that _____
who signed this certificate on behalf of the Contractor, was then _____
of said corporation; that said certificate was duly signed for and in behalf of said corporation by authority of its governing body, and is within the scope of its corporate powers.

(Corporate Seal)

(Signature and Date)

STANDARD FORM 328 (BACK) (4/1997)

CHANGED CONDITIONS: CERTIFICATE PERTAINING TO FOREIGN INTERESTS

You, as the FSO, should periodically check with appropriate company officials to be sure that you are aware of possible changes regarding FOCl. Whenever a change in the information reported on your facility's Certificate Pertaining to Foreign Interests is *anticipated*, submit a *letter report* of the anticipated change to your DSS Field Office. Whenever any change in the information reported on your facility's Certificate has *occurred*, submit a *new (revised) SF 328 Certificate* to your DSS Field Office. (1-302h(5), NISPOM). Contractors shall submit an updated SF 328 every five years **even if** the company reports no changes.

ORGANIZATION

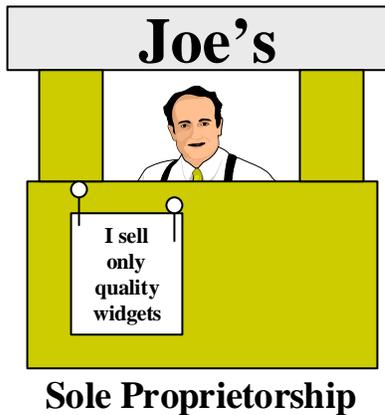
Identifying and assessing FOCl factors was an important part of clearing your facility. So too was sizing up the *domestic* sources of power affecting your facility. In the area of organization, this meant that DSS had to identify and assess any other entities that, by their relationship to your facility, could control or influence your facility's protection of classified information. During the initial survey, the IS Rep looked at your firm's basic documents to determine how your business was set up from a legal point of view.

As an FSO, you should be aware of your firm's current *business structure*. You should also be familiar with the other business structures (and of the FCL requirements for them) so that if your business structure changes you can report the change accurately to your DSS Field Office. So be ready to respond to the new requirements.

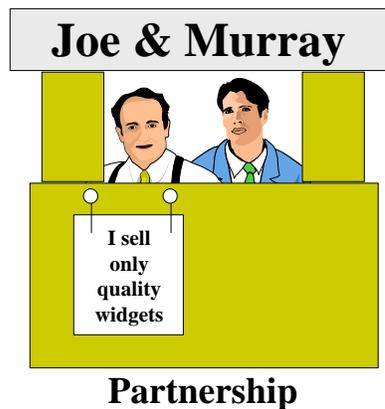
THE THREE BUSINESS STRUCTURES

These are three main types of business structures;

- the ***sole proprietorship***,
- the ***partnership***, and
- the ***corporation***.



The simplest type is the ***sole proprietorship***. In this type of business, one person owns and operates the business, sometimes with the aid of officers (a treasurer for instance) and executives (such as managers and supervisors). With a sole proprietorship, the owner ("proprietor") is the legal entity of the business, the party who is accountable in the eyes of the law for the business. When the owner becomes a NISP contractor, he or she is the party accountable for implementing the NISPOM requirements for the business.



The second type of business is the ***partnership***. With a partnership, the main partners, called "general partners," jointly own all of the firm's assets. These general partners are mutually accountable in the eyes of the law for the actions of the partnership. When the partnership is awarded a contract under the NISP, the general partners are mutually and severally (individually) accountable for implementing the NISPOM requirements for the partnership.



The third and most complex business structure is the ***corporation***. The corporation differs from the sole proprietorship and the partnership in that the owners of the corporation (stockholders) are *not* its legal entities. Instead, the corporation is considered to be itself an "artificial person" and thus a legal entity. With a corporation, the stockholders elect a Board of Directors who then appoint the principal officers of the corporation (usually a president, senior vice president, secretary, and treasurer). When a corporation is awarded a contract under the NISP, the Board of Directors and

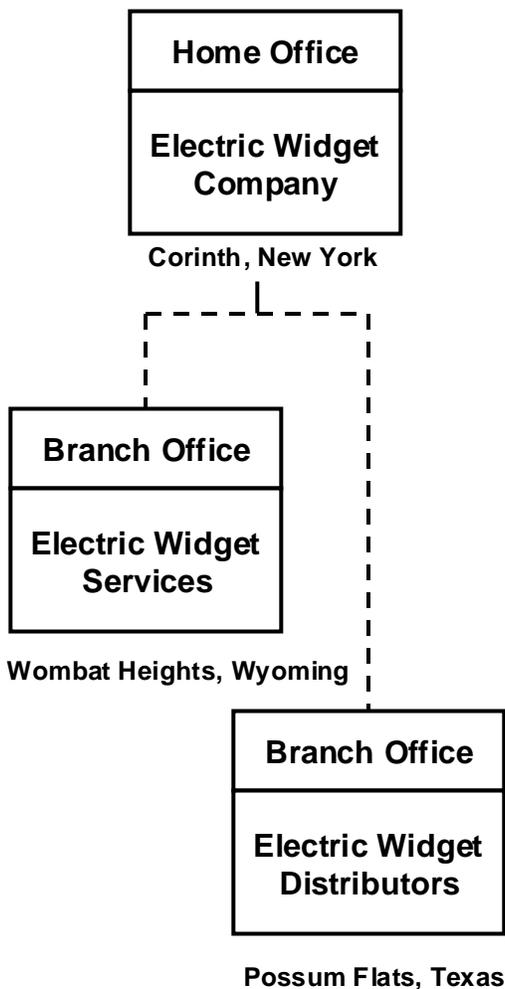
principal officers are accountable for the corporation in implementing the NISPOM requirements.

ORGANIZATIONAL STRUCTURES

A sole proprietorship, a partnership, or a corporation may confine its operations to one facility. In this case, just that one facility is studied during the processing for its clearance.

But there are two cases in which the clearance status (or “clearability”) of other facilities related to a facility being processed for an FCL is an issue. These two situations are the *Multiple Facility Organization (MFO)* and the *parent-subsidiary relationship*.

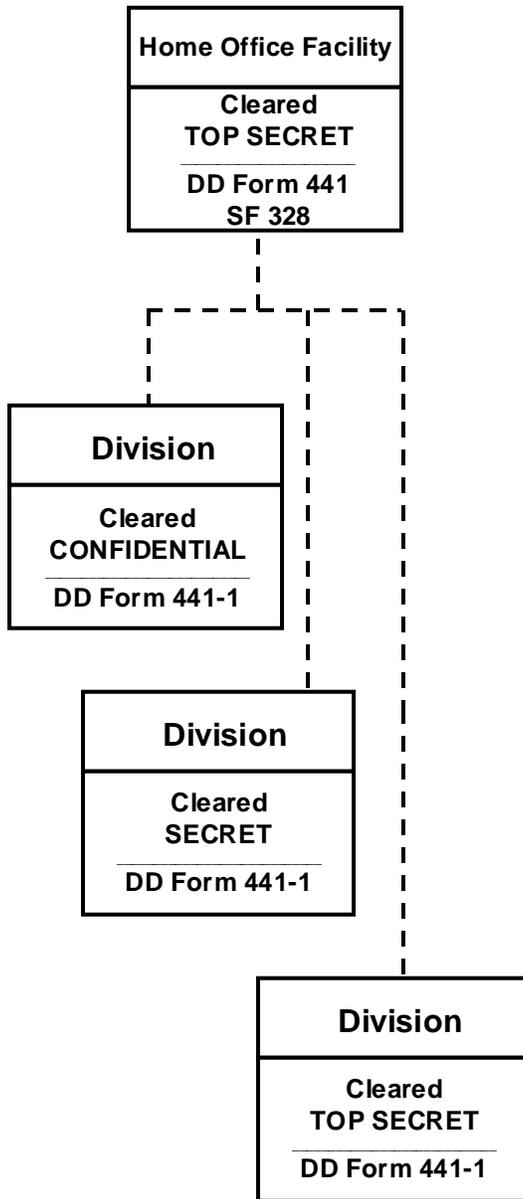
MULTIPLE FACILITY ORGANIZATION (MFO)



THE MULTIPLE FACILITY ORGANIZATION

Any of the three types of business structures; sole proprietorships, partnerships, and corporations (to include colleges and universities) may be configured (organized) as a Multiple Facility Organization (MFO). An MFO is a legal entity that is composed of two or more facilities.

For example: The corporate headquarters of the Electric Widget Company (EWC) is in Corinth, New York. EWC has two additional branch offices, one is the Electric Widget Services in Wombat Heights, Wyoming, and the other is Electric Widget Distributors in Possum Flats, Texas. Since the headquarters and the two branches together comprise a single legal entity, this corporation is an MFO.



MFO= 1 Legal Entity

The rule when clearing any subordinate facility of an MFO is quite simple. The home office (headquarters) facility, referred to as a HOF, must have a facility clearance of the *same or higher level than the subordinate facility*. The reason for the rule is also quite simple. The other facilities (divisions, branch offices, etc.) of the MFO are subordinate to the HOF, and their operations are usually quite closely linked. If the HOF were not cleared at the same or higher level, the HOF could have unauthorized access to the classified information available to a subordinate facility.

Since all of the facilities of an MFO together comprise a single legal entity, only the HOF can execute a Security Agreement (DD Form 441) with the U.S. Government. As required, subordinate facilities can be included in and covered by the HOF's Security Agreement by the execution of an *Appendage to the Security Agreement, (DD Form 441-1)*. A sample is shown on the next page.

Any FOCI elements at subordinate facilities must be included in the HOF's SF 328 (Certificate Pertaining to Foreign Interests).

As it happens, Electric Widget Services was cleared under a DD Form 441-1. Its HOF, the Electric Widget Company, Corinth, New York, had held a TOP SECRET facility clearance for several years. So when Electric Widget Services was awarded an Air Force contract to service widgets that are classified SECRET and are installed in aircrafts, EWS was included by the appendage (DD Form 441-1) to the existing Security Agreement.

APPENDAGE TO DEPARTMENT OF DEFENSE SECURITY AGREEMENT

Form Approved
OMB No. 0704-0194
Expires Jun 30, 2004

The public reporting burden for this collection of information is estimated to average 10 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0194), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS. RETURN COMPLETED FORM TO YOUR RESPECTIVE COGNIZANT SECURITY OFFICE.

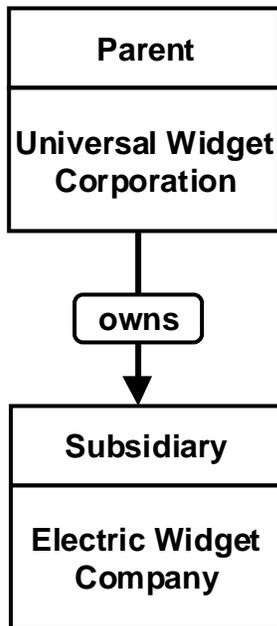
It is further agreed, on this _____ day of _____ by and between the United States of America through the Defense Security Service, acting for the Department of Defense, hereinafter called the Government, and _____ which has entered into the Security Agreement to which this appendix is made a part that the branches and/or facilities listed below, owned and/or operated by said contractor are included in and covered by the provisions of the said Security Agreement, and Certificate Pertaining to Foreign Interests, Standard Form 328.

NAME OF PLANT OR FACILITY	NUMBER AND STREET ADDRESS	CITY AND STATE

THE UNITED STATES OF AMERICA	CONTRACTOR <i>(Typed Name)</i>
BY <i>(Signature of Government Representative)</i>	BY <i>(Signature of Authorized Contractor Representative)</i>
AUTHORIZED REPRESENTATIVE OF THE GOVERNMENT <i>(Typed Name of Government Agency)</i>	TITLE <i>(of Authorized Contractor Representative)</i>
	ADDRESS

THE PARENT-SUBSIDIARY RELATIONSHIP

PARENT-SUBSIDIARY RELATIONSHIP



**Parent/Subsidiary =
2 Separate Legal Entities**

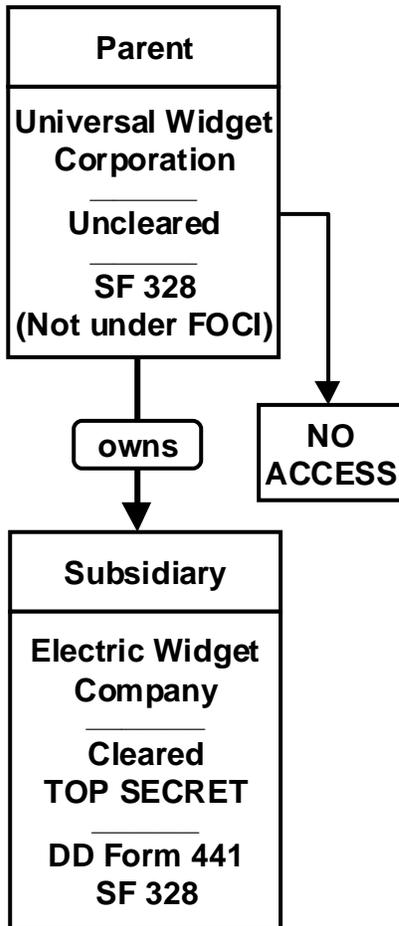
A *subsidiary* is a corporation that is controlled by another corporation. The controlling corporation is called a *parent*. (The parent controls the subsidiary through its ownership of over 50% of the voting stock of the subsidiary.) Because the parent controls the subsidiary, the general rule in the NISP is that the parent must have an FCL at the *same or higher level than the FCL of the subsidiary*.

But the parent-subsidiary 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 have a single legal entity, in a parent-subsidiary 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 hold an FCL of a higher level than the parent's FCL*.

In the first case, the Board of Directors of the parent formally excludes the parent from access to *all* classified information available to the subsidiary. Although the parent remains uncleared, the appropriate DSS Field Office ensures that the parent is not under FOCI or otherwise ineligible for an FCL.

In the second case, where the parent has an FCL, the Board of Directors of the parent formally excludes the parent from access to the classified information available to the subsidiary, *which is of a higher level than the level of the parent's FCL*. The subsidiary must then ensure that the parent is in fact denied access to the higher-level classified information.

Take the case of the Electric Widget Company (EWC). As we've noted, EWC has held a TOP SECRET facility clearance for years. EWC is a wholly owned subsidiary of the Universal Widget Corporation (UWC), an



international giant in the field of widgets. At the time when EWC was being processed for its TOP SECRET clearance, the Board of Directors of Universal Widget Corporation (the parent) excluded UWC from access to all classified information available to EWC (the subsidiary). Despite its multinational interests, UWC was found not to be under FOCI. Harold Huxtable, the FSO of EWC, after much consultation with his IS Rep, devised and implemented a remarkable SPP that has ensured over the years that none of the classified information accessed by EWC has ever been disclosed to its parent, UWC.

**CHANGED CONDITIONS:
ORGANIZATION**

Any time there is a change in the ownership or organization of your facility you must send a letter report to your DSS Field Office. For example, if your single-facility sole proprietorship becomes an MFO, or the owner takes a business partner, or the owner decides to incorporate, you must report the change to your DSS Field Office. If your firm is a corporation, and there are stock transfers that affect the control of the corporation, you must report the change. **(1-302h(1), NISPOM)**

KMP CLEARANCES



In addition to any organization factors affecting your facility's access to classified information, DSS took a careful look at the people in charge of your facility: its *Key Management Personnel* (KMPs). These include its owners, officers, directors, partners, regents, trustees, or executive personnel. The NISP recognized that your facility's top management and those who could control or influence their election, appointment, or tenure would have a direct impact on how classified information was protected at your facility. So it is essential to identify and individually clear your facility's KMPs *at the level of the FCL*.

Taking into account the different legal entities of the various business structures, as well as the particular circumstances at the facility, the IS Rep determines the KMPs requiring PCLs in connection with the FCL. Those KMPs that, as a general rule, must be cleared at the level of the FCL for each type of business structure are shown in the chart on the next page. Note that the management official in charge at the facility, and the FSO are the KMPs and must always be cleared. Based on their need for access, other KMPs may be cleared at the FCL level, cleared at a lower level, or excluded from being cleared. (2-104 and 2-106, **NISPOM**).



KMPs CLEARED at the FCL LEVEL



For a Sole Proprietorship:



- The owner.
- The management official in charge
- The FSO (who may be the owner)

Limited Liability Company (LLC):

- Managers
- FSO
- The management official in charge
- LLC members (must be either cleared or excluded)

For a College or University:



- The chief executive officer.

- Managerial group formally designated by the board of regents (or similar board) with authority and responsibility to negotiate, execute, and administer classified contracts.

- All regents, trustees, or directors unless they do not require access to classified information, do not occupy positions that enable them to adversely affect classified contract performance or have transferred their responsibility to a legal executive committee.
- The management official in charge.

For a Partnership:



- All general partners (unless there is a legal designated managing partner and/or legally constituted executive committee.

- All executive committee members (as long as the executive committee has been given full authority to act on behalf of the partnership)
- The management official in charge (if applicable).
- The FSO _____ **and** _____
- Other partners who occupy positions that enable them to adversely affect the partnership's policies or practices in the performance of classified contracts.

For a Corporation, Association, or Nonprofit Organization:

- The chairman of the board (if meetings are chaired by rotating chairman, all directors who fill the (rotating) chairman should be processed for a PCL. The issuance of the FCL will depend only on the issuance of the PCL for the current Chairman of the Board.)

- The senior management official e.g. chief executive officer (CEO) or president.
- The FSO.
- Concurrent PCLs are not needed for KMPs that are cleared with another cleared facility within a corporate family. (MFO or parent/subsidiary)
- KMP listing should indicate which facility within the corporate family holds the PCL.

When the Electric Widget Company was processed for its TOP SECRET clearance, its KMPs were (and still are):

- J. Digby Wilbersnoot, who serves as both Chairman of the Board and President of EWC. (EWC has never had a chairman *pro-tem* or a rotating chairman of its board. As J.D. is fond of saying, "There's nothing temporary about *this* chairman.")
- Harold Huxtable, Senior Vice President and Facility Security Officer.
- After consultation and concurrence with the IS Rep., Alice Malarkey, Vice President in charge of Public Relations, Viola Wilbersnoot, Treasurer and board member, and Melvin Overcoat, Secretary and board member for EWC were excluded from access to classified information by the board of directors and therefore did not need a personnel clearance. If these officers require access to classified information they may be processed concurrent with the FCL but the FCL determination is not contingent upon the status of their PCL.

When Electric Widget Services was being cleared, there were only two KMPs to be cleared, since it was a branch office of EWC:

- Walter Wilbersnoot, the Branch Manager at EWS.
- Harriet Hornsby, the Assistant Branch Manager and Facility Security Officer.

CHANGED CONDITIONS: *KMP CLEARANCES*

Change in KMPs. You must submit a report to your DSS Field Office of any change in your facility's KMPs, such as a KMP leaving your company and/or a new KMP coming on board. In the case of a new KMP, you need to state in your report the name of the person that the KMP is replacing (if applicable); whether or not the new KMP is cleared (and if so, to what level and when); and the new KMP's date and place of birth, social security number, and citizenship. You must also state whether the new KMP has been formally excluded from access to classified information under 2-106 of the NISPOM (with the concurrence of the IS Rep), or whether the KMP has been temporarily excluded from access pending the granting of a PCL. (1-302h(3), NISPOM)

KMP RFIs. You must submit a report to DISCO (with a courtesy copy to your DSS Field Office) if a KMP becomes a Representative of a Foreign Interest (RFI) or if the KMP's status as an RFI changes in a manner that would make the KMP ineligible for a personnel clearance (see 1-302d, NISPOM); include the RFI statement (see 2-209b, NISPOM).

LETTER OF NOTIFICATION OF FACILITY SECURITY CLEARANCE

DISCO will send your facility a Letter of Notification of Facility Security Clearance (DSS FL 381.R) when your facility has successfully fulfilled these five essential elements:

- When it had been properly sponsored;
- When it had executed a Security Agreement;
- When, if applicable, its home office or parent had been properly cleared or, if allowed, excluded;

- When it had been determined not to be under FOCI;
- When its KMPs had been properly cleared or, if allowed, excluded - only then did DISCO issue your facility a ***Letter of Notification of Facility Security Clearance (DSS FL 381-R)***.

SUMMARY

The Facility Security Clearance is a means of assessing the suitability of a contractor to be trusted with access to classified information. To be cleared, a facility must meet requirements in five areas: sponsorship, Security Agreement, Certificate Pertaining to Foreign Interests, organization and KMP clearances. Changed conditions affecting the facility clearance must be reported to the DSS Field Office as required by 1-302h of the NISPOM.

3b - Review Exercises

Complete the following exercises for review and practice.

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



1. The general rule is that a facility that is determined to be under FOCI is ineligible for a facility clearance.
 True. False.
2. A facility is determined to be under FOCI when any foreign ownership, control, or influence of the facility exists.
 True. False.
3. Whenever a significant change has occurred that affects the information reported on your facility's Certificate Pertaining to Foreign Interests (SF 328), you must
 a. report the change to DSS Headquarters.
 b. report the change to DISCO.
 c. report the change to your DSS Field Office.
 d. submit a revised Certificate to your DSS Field Office.
4. With a sole proprietorship, the owner is the legal entity of the business and as a NISP contractor, is accountable for implementing the NISPOM requirements that apply to the business.
 True. False.

5. Match the descriptions with the "5 essential elements."

	Element	Description
_____	Sponsorship	a. The facility submits information, which is the basis for determining whether or not it is under FOCI.
_____	Security Agreement (DD Form 441)	b. The facility's top management and those who could affect their selection or tenure are identified and individually cleared or formally excluded
_____	Certificate Pertaining to Foreign Interests (SF 328)	c. General policy calls for a controlling facility to have an FCL at the same or higher level than the controlled facility.
_____	Organization	d. A User Agency or contractor thereof requests that DISCO initiate a facility clearance action.
_____	KMP clearances	e. The U.S. Government and the contractor sign a standard contract that binds the facility's management to the provisions of the NISPOM.

6. With a partnership, the general partners are the legal entities of the business and, when the partnership is a NISP contractor, the general partners are accountable for implementing the NISPOM requirements that apply to the business.

True. False.

7. With a corporation, the corporation is itself the legal entity and, when the corporation is a NISP contractor, its Board of Directors and principal officers are accountable for the corporation in implementing the NISPOM requirements that apply to the business.

True. False.

8. A Multiple Facility Organization (MFO) is a legal entity that is composed of two or more facilities.

True. False.

9. In general, a Home Office Facility (HOF) of an MFO must be cleared at the same or a higher level than a division in order for the division to be granted a facility clearance.

True. False.

10. Subordinate facilities (e.g., divisions or branch offices) of an MFO are included in and covered by the HOF's Security Agreement by the execution of an appendage form (DD Form 441-1).

True. False.

11. As part of their processing for FCLs, subordinate facilities of an MFO must each complete a Certificate Pertaining to Foreign Interests (SF 328).

True. False.

- 19.** For a college or university, the KMPs usually cleared at the level of the FCL are
- a. the chief executive officer.
 - b. Other officers or officials specially and properly designated by action of the board of regents as the managerial group with authority and responsibility for the negotiation, execution, and administration of classified contracts.
 - c. all regents, trustees, or directors who could sit as *pro-tem* or rotating chairman of the executive body.
 - d. all deans and department heads.
 - e. the management official in charge at the facility.
 - f. the FSO.
- 20.** You must submit a letter report to the DSS Field Office whenever there is a change in your facility's KMPs, such as a KMP leaving your firm or a new KMP joining your firm.
- True. False.
- 21.** You must submit a report to DISCO whenever one of your facility's cleared KMPs becomes a Representative of a Foreign Interest (RFI) or when the status of a KMP who is an RFI changes so as to make the KMP ineligible for a personnel security clearance.
- True. False.

3b - Solutions & References



1. True. (p. 3-19).
2. False. (p. 3-19).
3. d and c. (p. 3-24).
4. True. (p. 3-25).
5.
 - d. Sponsorship. (p. 3-4).
 - e. Security Agreement (DD Form 441). (p. 3-6).
 - a. Certificate Pertaining to Foreign Interests (SF 328). (p. 3-22).
 - c. Organization. (pp. 3-24-27).
 - b. KMP clearances. (p. 3-33).
6. True. (p. 3-25).
7. True. (pp. 3-25).
8. True. (p. 3-26).
9. True. (p. 3-27).
10. True. (p. 3-28).
11. False. (p. 3-27).
12. parent, subsidiary. (p. 3-29).
13. a., c., d. (p. 3-29-30).

- 14.** Key Management Personnel. (p. 3-31).
- 15.** True. (p. 3-31).
- 16.** a. (p. 3-31).
- 17.** True. (p. 3-25).
- 18.** b., d. (p. 3-25).
- 19.** a., b., c., e., f. (p. 3-32).
- 20.** True. (p. 3-34).
- 21.** True. (p. 3-34).

LESSON 4

Personnel Security Clearances General Concepts

In this lesson we'll examine the Industrial Personnel Security Clearance Program. This is a program to "clear" employees at industrial facilities for access to classified information when they need access to do their jobs. We will look briefly at who determines clearances and on what grounds. There will also be a section on what the FSO, can do to prevent delays in the clearance process. Finally, we will discuss the ways in which a clearance may be terminated.

OBJECTIVES

When you finish this lesson you should be able to do the following:

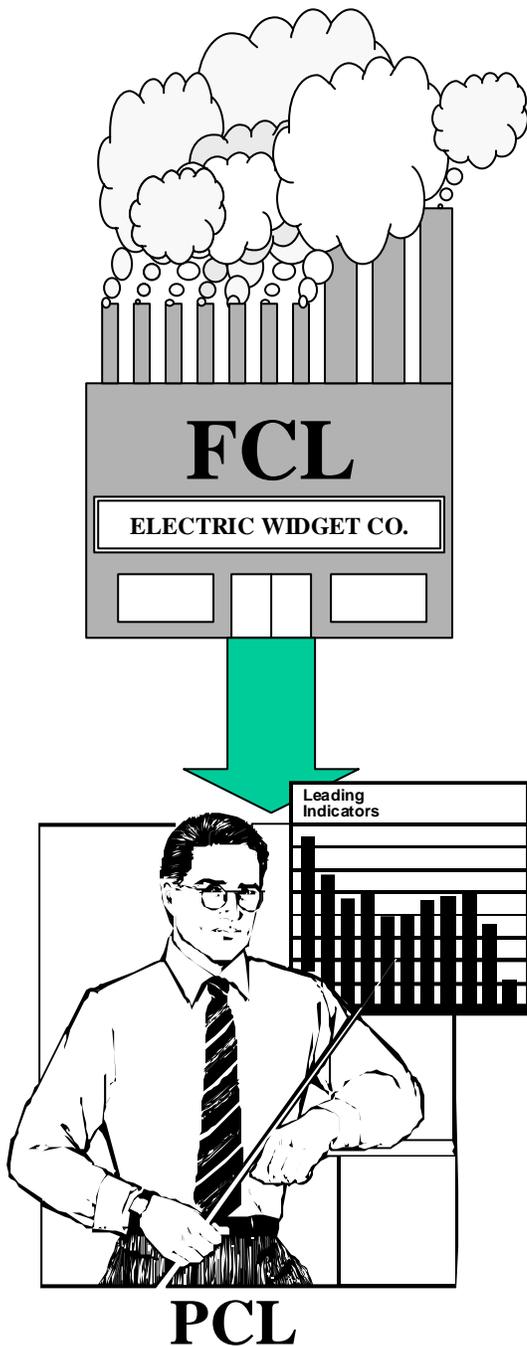
- Define a Personnel Security Clearance (PCL).
- Explain briefly the roles of the Defense Security Service, DISCO and the Defense Office of Hearings and Appeals (DOHA) in the granting, revocation, and denial of PCLs.
- Describe the general criteria for granting PCLs.
- Explain the ways in which you, the FSO, may aid in the process of clearing employees at your company.
- Differentiate clearance denial, suspension, revocation, and termination.

PERSONNEL SECURITY CLEARANCES

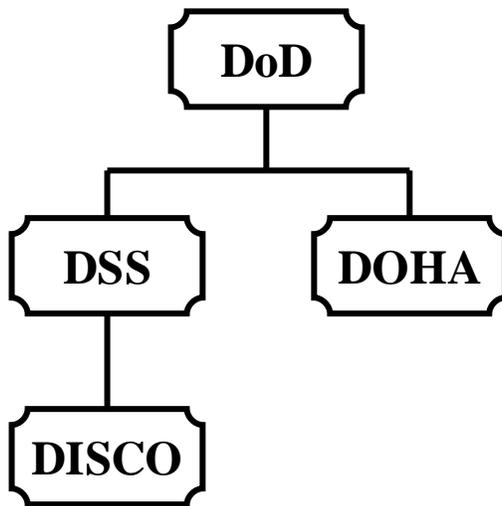
In the last lesson we discussed the reasons and procedures for the granting of Facility Security Clearances (FCL). One of the main reasons for a FCL was, however, touched upon lightly. That reason is people. A Facility Security Clearance is granted to allow the clearing of employees who have a need to handle classified information, either in the facility itself, at another cleared facility, or at a government installation. Where necessary, the approval of a facility for storage of classified information may be granted.

What is a Personnel Security Clearance? A Personnel Security Clearance (PCL) is "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 PCL being granted" (**Appendix C, NISPOM**). In other words, a PCL is ***a determination or prediction that an individual can be relied on to safeguard our national secrets.***

This is an important concept. The Personnel Security Clearance is not a piece of paper. It is a determination, essentially an educated guess, as to a person's character. And the issuance of a "final" clearance is *not* the final word on that person's character. The PCL philosophy allows for the possibility of inaccuracy in the original determination or prediction and also for the changes in a person's character over time. So continuing evaluation is called for. As part of this continuing evaluation, the government conducts periodic reinvestigations on cleared personnel. The level of the individual's clearance determines the frequency and depth of these investigations.



OGC and DOHA



Who makes the clearance determination or prediction? The determination is made by the Department of Defense at one of two levels. Favorable determinations may be made at the DSS *Defense Industrial Security Clearance Office (DISCO)* or, if further deliberation is required, the determination is made at the *Defense Office of Hearings and Appeals (DOHA)*. A favorable determination from either office prompts DISCO to issue an electronic *Letter of Consent (LOC)*, which informs the FSO that the applicant has been granted a clearance to a specified level. Again, this is not the clearance itself, only a notification. All denials and revocations of Personnel Security Clearances come from DOHA. DISCO is within the structure of the Defense Security Service. DOHA belongs to the DoD's Office of the General Counsel.

What is the clearance determination based on? The determination or prediction of the person's trustworthiness is based on some form of investigation. The nature and extent of the investigation is determined by the level of clearance required by the employee. There are three basic levels of classified information: **TOP SECRET**, **SECRET**, and **CONFIDENTIAL**. When an **Interim clearance** is granted to an employee, the access to classified information is more restrictive than a **FINAL Clearance** in terms of what information the holder is permitted to access. Interim **SECRET** and **CONFIDENTIAL** clearances granted by the Cognizant Security Agency (CSA) are valid for access to classified information at the level of the interim PCL. However, an Interim Clearance granted at the **SECRET** or **CONFIDENTIAL** level is not authorized for access to the following:

- Sensitive Compartmented Information
- Restricted Data (RD)
- COMSEC (Communications Security) Information
- SAP (Special Access Programs)
- NATO Information (See note on next page)

The Six Functions of DISCO

- Determine eligibility of applicants
- Initiate appropriate investigations
- Review investigative findings
- Refer doubtful cases to DOHA for adjudication
- Issue Letters of Consent (LOCs)
- Keep records of PCLs and

An interim **TOP SECRET Clearance** is valid for access to RD, COMSEC and NATO Information at the **SECRET and CONFIDENTIAL** level only.

NOTE: The following applies to NATO information:

Operation **ENDURING FREEDOM** has created a particular need to ensure timely access by involved operational commands and other activities to NATO classified. Accordingly, for the duration of **ENDURING FREEDOM**, contractor & military personnel with established need-to-know, that have been granted an interim PCL, are eligible for access to NATO information of the equivalent level of classification. Access to COSMIC TOP SECRET, COSMIC TOP SECRET ATOMAL information **is not authorized**. Access to NATO classified material for interim PCL's shall be subject to the following conditions:

- Approval by the authority who is granting access to U.S. classified information based on the interim security PCL.
- Written authorization, maintained as a record.
- Interim PCL held at the SECRET or TOP SECRET level
- Process for a final security clearance has been initiated
- Individual has received and acknowledged a briefing on NATO security requirements.

(As stated in the Office of the Under Secretary of Defense Memorandum, dated 4 Dec 01, SUBJECT: Facilitating Necessary Access to NATO Classified Information.)

Immigrant aliens and foreign nationals are not eligible for PCLs, but in special cases they may be granted a **Limited Access Authorization (LAA)** at the SECRET or CONFIDENTIAL level, as required. Many restrictions apply to LAAs; these restrictions are spelled out on charts in the next lesson.

PERSONNEL SECURITY INVESTIGATIONS



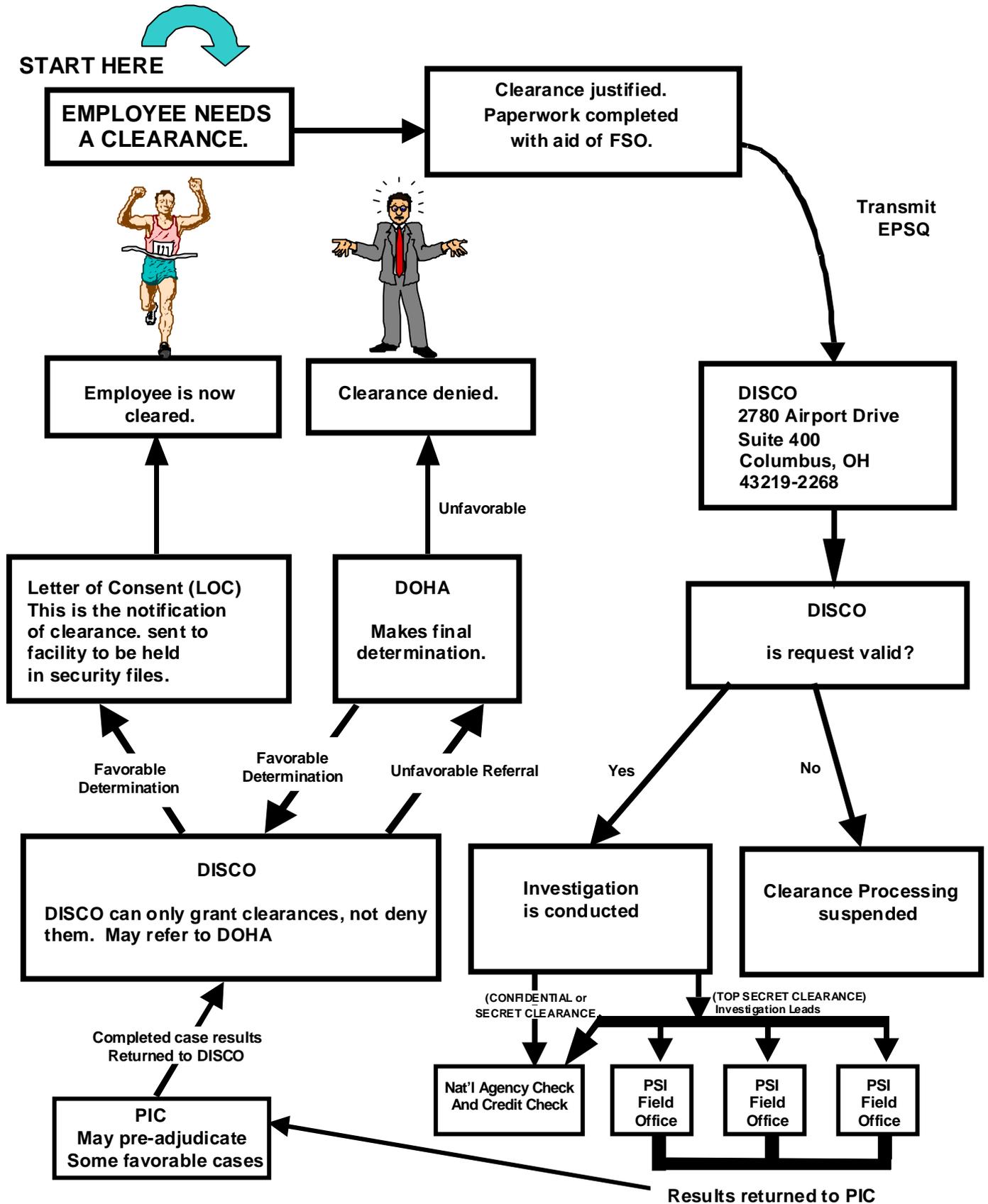
Special Agent's Badge



A National Agency Check with Local Agency Check and Credit Check (NACLC) is the basic investigative requirement for a SECRET or CONFIDENTIAL clearance. A Single Scope Background Investigation (SSBI) is required for a TOP SECRET clearance. Employees of the Defense Security Service or investigators representing the office of Personnel Management (OPM) carry out the actual investigations of applicants for clearances.

Essentially their job involves "running leads," that is, checking out references and records as indicated by the information on the Electronic Personnel Security Questionnaire (EPSQ) completed by the applicant for a security clearance. In many instances, they also conduct Subject Interviews with applicants.

LIFE CYCLE OF A PERSONNEL SECURITY INVESTIGATION



RIGHTS AND RESPONSIBILITIES OF CLEARED PERSONNEL

While being evaluated for a Personnel Security Clearance, an employee is entitled to the provisions of due process. These provisions, stated in Executive Order 12958, Access to Classified Information, mandate that a PCL cannot be denied or revoked unless an individual is given the following:

- A written explanation of the basis for the denial or revocation of the clearance.
- Any documents, records, and reports upon which the denial or revocation is based if they would be made available under the Freedom of Information Act or Privacy Act.
- An opportunity to be represented by legal counsel.
- A reasonable opportunity to reply to and request a review of the determination.
- Written notice of and reasons for the results of the review, the identity of the deciding authority, and written notice of the right to appeal.
- An opportunity to appeal in writing to a high level panel appointed by the agency head.
- An opportunity to appear personally at some point in the process before a government authority other than the investigating authority.

Bear in mind, no one has a right to a PCL. A person does have the right to a formal and impartial review of why a PCL is to be denied or revoked.

Along with the PCL the employee acquires the responsibility to protect classified information. *The employee learns the details of this protection through you, the FSO.* This knowledge comes through a number of methods: briefings, the SPP you may have prepared, memos, and many other ways. But ultimately, the responsibility rests with that employee. If the holder of a PCL is unable or unwilling to protect classified information, the NISP is undermined and national security threatened.

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 be a basis for denial of clearance.

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.

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 obligation 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. Contacts 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.

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.

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 judgment 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.

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 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.

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.

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.

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.

Guideline J: Criminal conduct

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

Guideline F: Financial considerations

Personnel Security Clearance *Eligibility Criteria*

Guideline K: Security Violations

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

Guideline L: Outside activities

The Concern: Involvement in certain types of outside employment or activities is 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.

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.

These guidelines are published as Appendix A. of the Department of Defense (DoD) Personnel Security Regulation (DoD 5200.2R)

FSO RESPONSIBILITIES

While the basic responsibility for protecting classified information rests with the cleared employee, the FSO has the task of educating that employee, keeping PCL related records, and submitting timely reports on changes affecting PCLs.



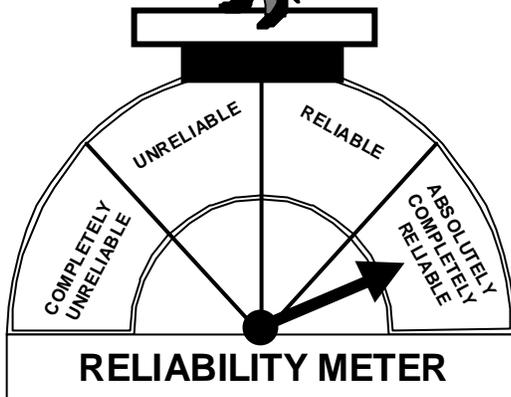
There is much the FSO can do to speed up the PCL process to save time for both the FSO and the government. The most obvious way to shorten the PCL process is *not to use the process unless it is absolutely necessary*. Does the employee really need a clearance, or is the request based on status-seeking, over-enthusiastic contingency planning, as a pre-employment screening tool, or some other such consideration? Reducing the number of clearances is a major goal within the NISP, and IS Reps will be scrutinizing this area during every visit.

This goal of clearance reduction and the avoidance of unnecessary clearances have been incorporated into the NISPOM itself and should be included in your SPP. The SPP should outline your facility's system for limiting personnel security clearances. The essential elements of this system are identification for those who are required to make decisions on a person's *need* for a clearance and those who review that decision. These elements are set within the framework of maintaining the minimum number of clearances necessary to meet contractual obligations. The appropriateness of the numbers and levels of PCLs at your facility will be assessed during reviews and other visits to your facility by the Field Office, based on the needs established by your classified contract.



By submitting a clearance application on behalf of an employee, you are essentially saying that certain prerequisites have been met. DSS depends on you, the FSO, to ascertain the citizenship of the applicant through the viewing of proper documentation; if the applicant is a representative of a foreign interest; if the applicant has had a prior clearance; to provide adverse information if known; and so forth.

The NISPOM Chapter 2, Section 2 provides guidance related to Personnel Security Clearance.



FSO RESPONSIBILITIES AFTER THE PCL HAS BEEN GRANTED

Your responsibility to the employee does not end with the submission of the clearance application papers. The granting of a clearance is only part of the equation. The other part is security education. Immediately this means an "initial briefing," a summary of which may be found in paragraph **3-106** of the NISPOM. Following the initial security briefing, a **newly cleared employee** must read, understand, and sign the SF 312 (Classified Information Non-Disclosure Agreement) **prior to having access to classified information**. Employees that held a previous PCL that was converted or reinstated in accordance with NISPOM paragraphs 2-215 and 2-217 need not sign an additional SF 312, if a record exists showing that they have already signed one. The briefings associated with the security education of cleared employees are discussed in Lesson 8.

DENIAL



Zebediah Smythe applied for a clearance, but was denied due to issues uncovered in the clearance process.

SUSPENSION/ REVOCATION



Denise “Fingers” Malone was caught pocketing a piece of classified hardware. Her SECRET clearance was immediately suspended and subsequently revoked.

ADMINISTRATIVE TERMINATION



Duncan Undersides no longer works on any classified projects. While he continues to work at EWS, his clearance is not necessary so Harriet administratively terminated Duncan’s clearance.

DENIAL

Four official actions lead to an employee *not* holding a Personnel Security Clearance. One is the *denial* of the PCL based on the initial application. In this case, the applicant is deemed unworthy of the clearance based on unfavorable information and the clearance is not issued.

SUSPENSION AND REVOCATION

The other three actions involve an existing clearance. With a *suspension* or *revocation*, as with a denial, the employee is found to be ineligible for the clearance. This finding may be based on a periodic reinvestigation, an adverse information report resulting in a reinvestigation, a report of compromise traced back to an individual, or some other cause. Suspension may end in restoration of access or in revocation of the clearance. The person is usually reinvestigated before the clearance is revoked.

CLEARANCE TERMINATION

Denial, suspension, and revocation are all entirely government determinations. The remaining action, the *clearance termination*, is determined primarily by the contractor. This action does not reflect on the worthiness of the employee. Rather, it is based on the lack of continued need for the clearance. Through clearance terminations, the government is able to cut back on the huge number of cleared personnel, thus eliminating the time and money spent on periodic reinvestigations and files maintenance for unneeded clearances. In a clearance termination, the employee (1) terminates from your company, or (2) continues to work at your company, either on another project or perhaps on unclassified parts of the same project. The chart on page 5-29 gives a brief run-down of the procedures on the part of the contractor (FSO) for terminating clearances.

SUMMARY

A Personnel Security Clearance (PCL) is 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 PCL being granted. A National Agency Check with Local Agency Check and Credit Check (NACLIC) is the basic investigative requirement for a SECRET or CONFIDENTIAL clearance. A Single Scope Background Investigation (SSBI) is required for a TOP SECRET clearance. When findings are acceptable, DISCO issues a Letter of Consent to notify the facility that a personnel clearance has been granted. Although being granted a PCL is not a right, an applicant for a PCL is entitled to the provisions of due process if a clearance is denied. The determination to deny a PCL is made by DOHA. Once granted, a PCL remains subject to revocation by DOHA. When a PCL is no longer required, it must be terminated. FSOs must ensure that clearance applications are submitted only when necessary, that they are accurate and complete, that PCL records are properly maintained, and cleared employees are educated in their security responsibilities.

How to Avoid Delays

- Request only essential clearances.
- Use the Electronic Personnel Security Questionnaire (EPSQ).
If you cannot use electronic version, contact your IS Rep.
- Ensure, as far as possible, through a careful review that all forms are completed fully and correctly.
- Be sure to address all mailings correctly.
- Prepare and submit packets promptly .

4 - REVIEW EXERCISES

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



1. A Personnel Security Clearance (PCL) is an a_____
d_____ that an individual is eligible, from a security point of view,
for a_____ to c_____
i_____ of the same or lower category as the level of PCL being
granted.
2. In its processing of an individual for a PCL, DISCO either makes a favorable
determination and grants the PCL or refers the case to DOHA for a final determination.

 True False
3. Only DOHA is authorized to deny or revoke a PCL.

 True False
4. Both DISCO and DOHA are components of the Defense Security Service.

 True False
5. The official notification that a PCL has been granted is called a L_____ of
C_____.

- b. _____
- c. _____
- d. _____

8. Match the descriptions with the PCL actions. Descriptions may apply to more than one action.

PCL Actions		Descriptions
_____	Denial	a. usually entails a reinvestigation of the cleared person.
_____	Suspension	b. determination made primarily by the contractor.
_____	Revocation	c. determination made entirely by the government.
_____	Clearance Termination	d. action taken when a cleared person no longer requires a clearance. e. due process is followed. f. based on issues related to initial application for clearance. g. individual is deemed ineligible for the clearance.

4 - SOLUTIONS & REFERENCES



1. Administrative determination, access, classified information. (p. 4-2).
2. True. (p. 4-3).
3. True. (p. 4-3).
4. False. (p. 4-3).
5. Letter of Consent. (p. 4-3).
6. Your description should include the following points: Honesty, good judgment, reliability, and trustworthiness. (p. 4-8).
7. See the four ways listed on (p. 4-10 & 4-13)
8. c, e, f, g Denial.

c, g Suspension.

a, c, e, g Revocation.

c, d, e, g Clearance termination.

(pp. 4-6, 12).

**USE THE
DEFENSE**

HOTLINE

**TO REPORT FRAUD, WASTE,
& SECURITY VIOLATIONS
RELATING TO
DOD CONTRACTS.**

800/424-9098-toll free

hotline@dodig.osd.mil or www.dodig.osd.mil/hotline



**OR WRITE:
DEFENSE HOTLINE
THE PENTAGON
WASHINGTON, D.C.
20301-1900**

**IDENTITIES OF WRITERS & CALLERS
FULLY PROTECTED.**

LESSON 5

Personnel Security Clearance Procedures

This lesson provides a section of charts to help you determine which procedures and forms are needed for employees that require a Personnel Security Clearance (PCL) or a limited access authorization (LAA). These charts are based both on the level of clearance required and the status of the employee, and cover almost a full range of cases. After the charts, you will find some samples of completed clearance applications. Finally, there is a chart listing the procedures for termination of PCLs and LAAs.

We'll be using the employees of Electric Widget Services and its Home Office Facility (HOF), the Electric Widget Company, to illustrate the procedures involved.

JOINT PERSONNEL ADJUDICATION SYSTEM (JPAS)

The Joint Personnel Adjudication System (JPAS) comprised of The Joint Clearance and Access Verification System (JCAVS) and Joint Adjudication Management Systems (JAMS) is currently being beta tested. JPAS is the system of the **future** that will handle **all** of the current paper transactions (relative to PCL's) electronically and in **real time**. Actions will include but not be limited to actions that currently involve the use of DISCO Form 562. Some examples of actions that will be done electronically when the JPAS system is fully implemented are terminations, upgrades, downgrades, reinstatements and maintaining non disclosure signature dates. The Joint Clearance and Access Verification System (JCAVS) which is one facet of the JPAS, will be

used extensively by DoD contractors participating in the National Industrial Security Program (NISP). For further information, contact your local DSS Industrial Security Representative. You may also find information about JPAS at: <https://jpas.osd.mil>, and the DoD Industrial Security Letter (ISL) 02L-1, dated 22 April 2002.

OBJECTIVES

When you finish this lesson you should be able to do the following:

- Using the charts provided, follow the procedures for preparing applications for PCLs and LAAs.
- State some tips and hints in successfully using EPSQ.
- Explain how unnecessary PCLs and LAAs are terminated.

HOW TO READ THE CHARTS



Wanda Fishtank

The charts on the following pages provide a guide for you, the FSO, in determining what actions to take in preparing a clearance application packet to be forwarded to DISCO. Don't be discouraged by all the boxes. You need only read through those areas that apply to the clearance you are checking on.

Take, for example, Wanda Fishtank of Electric Widget Services (EWS). If her supervisor should come to Harriet Hornsby's office (Harriet is EWS's FSO) saying she required a SECRET level clearance, all Harriet need do is turn to the charts and begin to read down through the various conditions. Those conditions that do not apply are disregarded. The first two pages of the charts cover general requirements: Is the clearance warranted? After a bit of research, Harriet decides that Wanda's duties will require her to have access to SECRET information. Is she a US citizen? Yes, and she provides a passport to prove it. Has she ever had a clearance before? No, so Harriet can now turn directly to Chart 10

page 5-13 and follow the steps for preparing a SECRET clearance application.

On the pages following the charts we have provided additional examples of EWC personnel to help you "walk through" the process. These examples will give you a better idea of the various clearance situations. The pages with the charts are numbered separately to simplify their use.

Chart 1



General Requirements

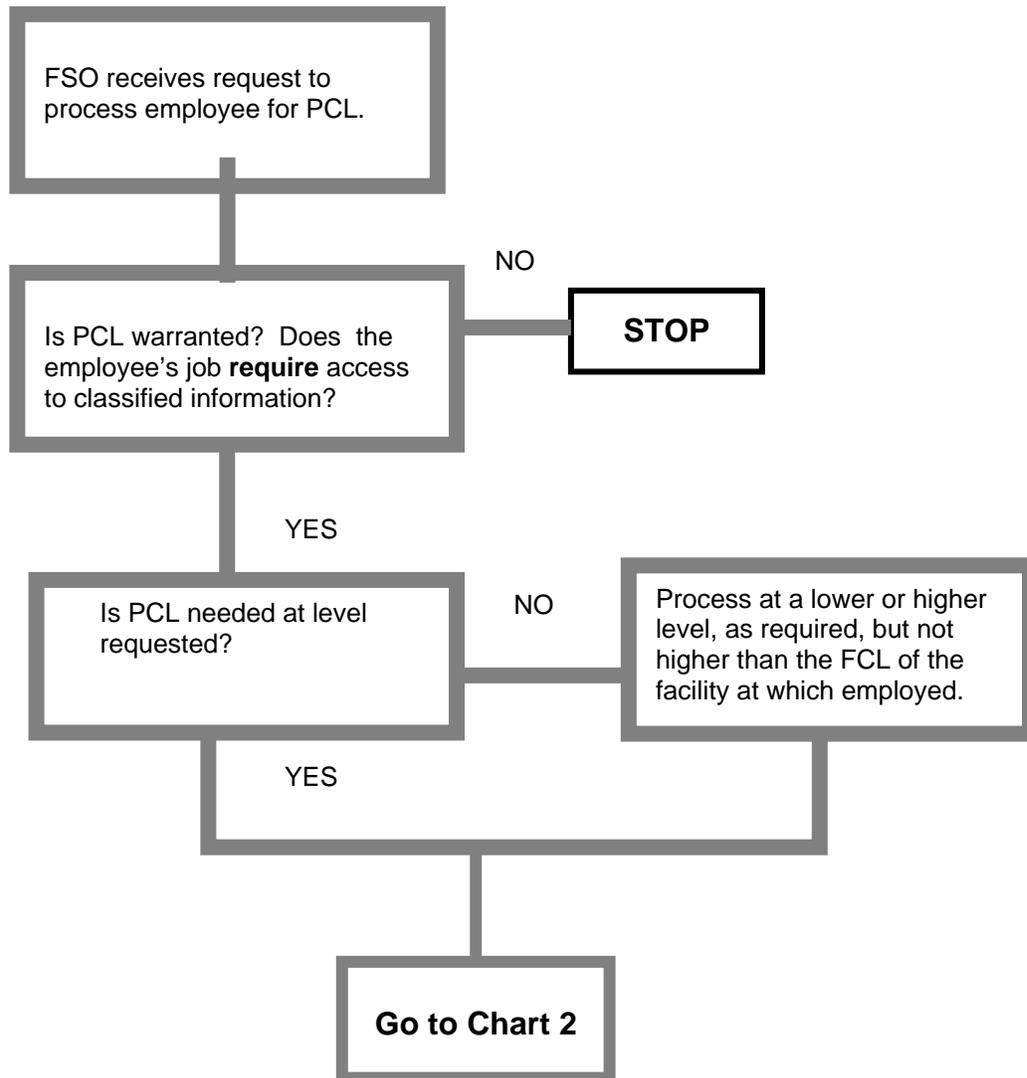


Chart 2



General Requirements (cont'd)

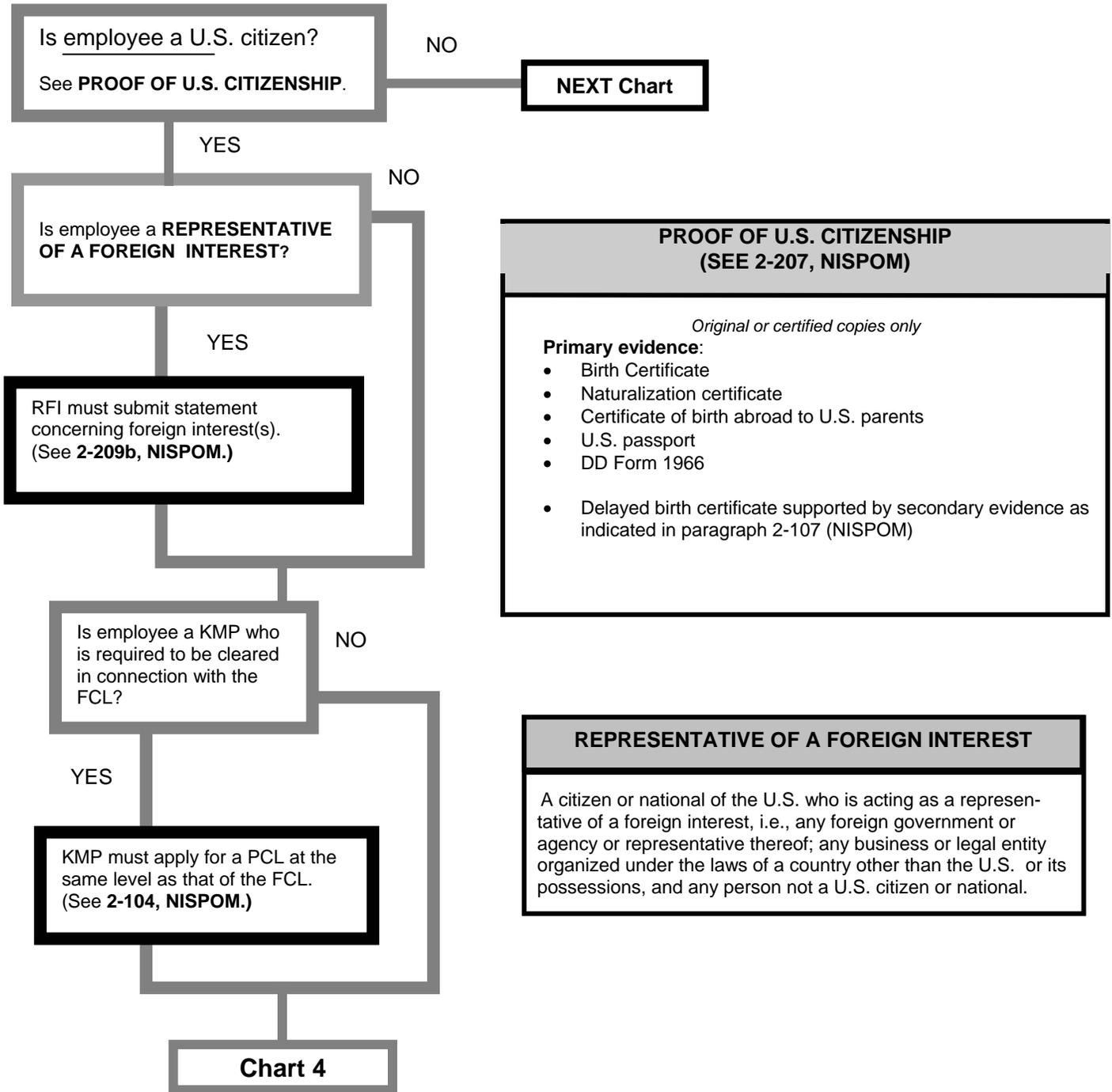


Chart 3



Non-U.S. Citizens: Limited Access Authorization

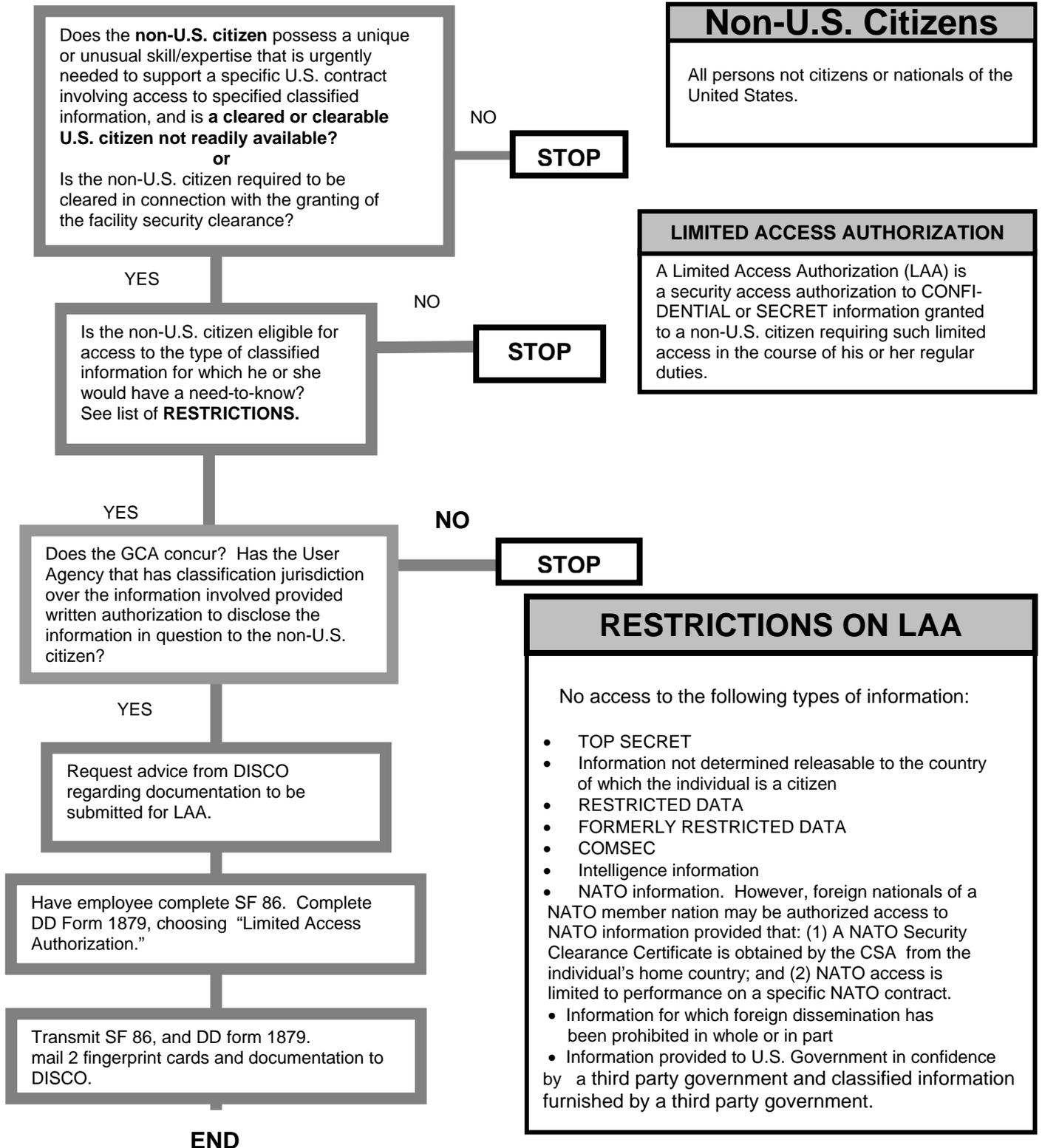
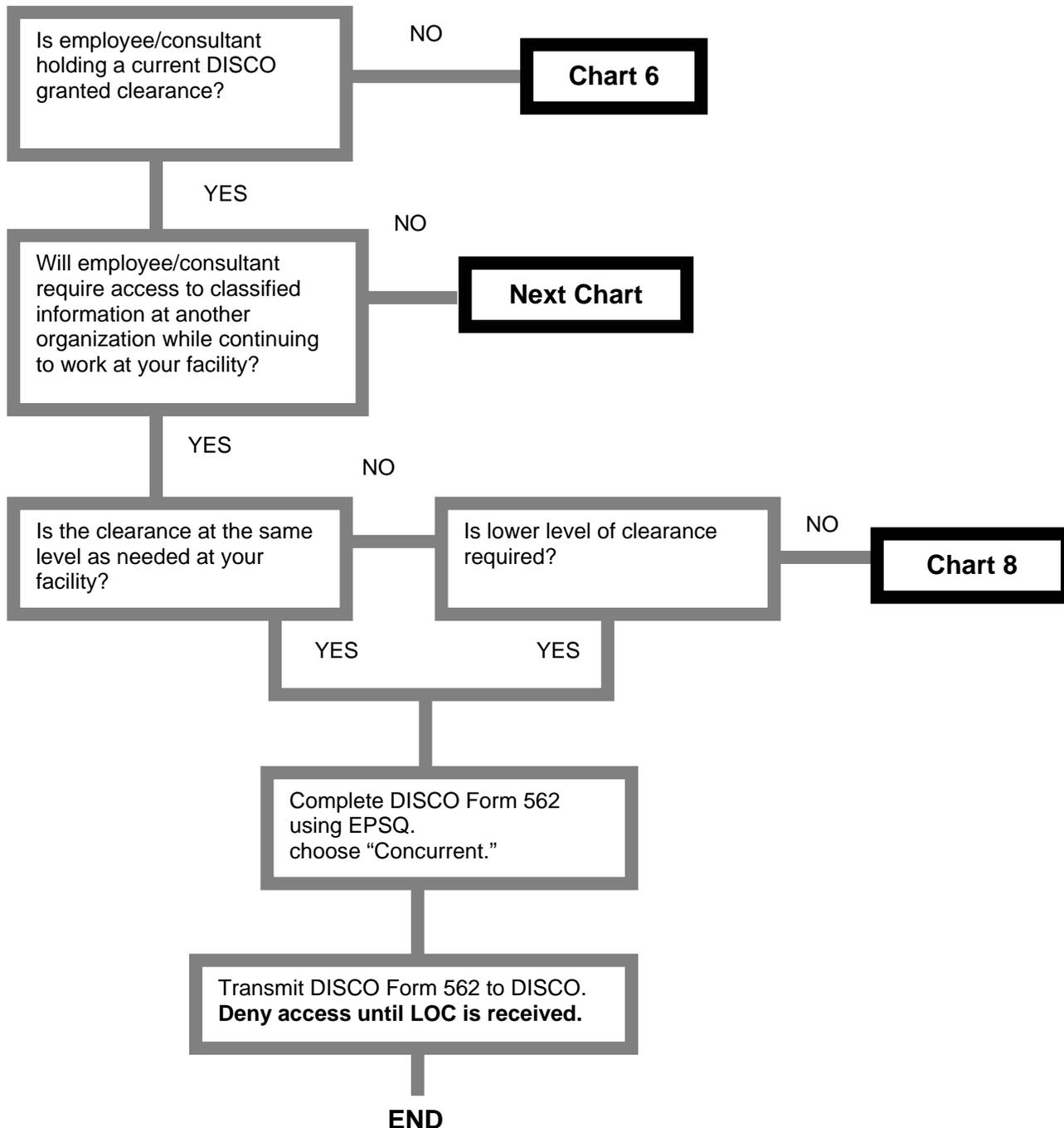


Chart 4



Concurrent Clearance



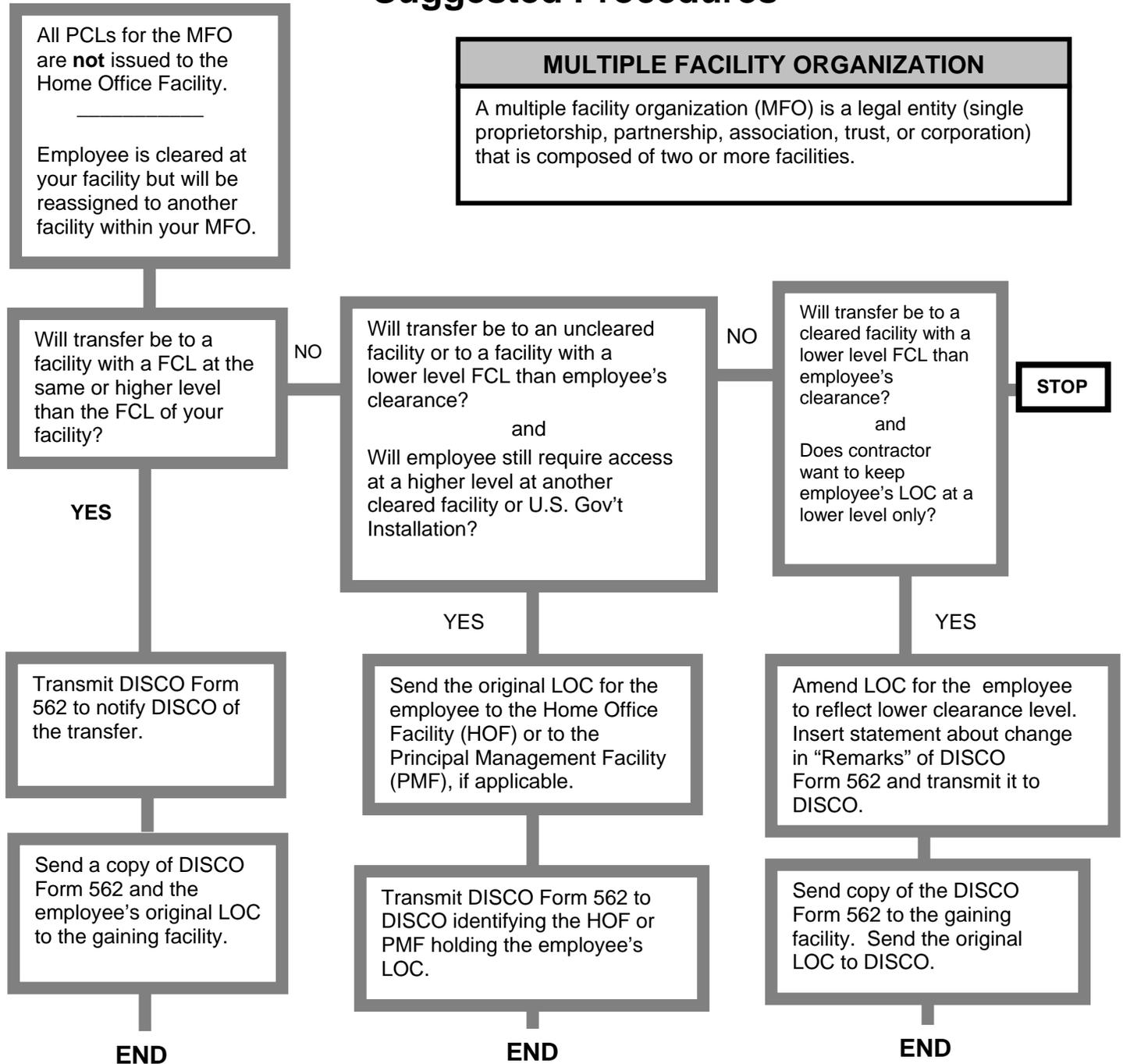
NOTE: An LOC (Letter of Consent) is an electronic transmission that DISCO sends to the contractor that indicates the level of the Personnel Security Clearance (PCL) and date of the PCL.

Chart 5



Clearance Transfer Within a Multiple-Facility Organization when all PCLs *not* Issued to HOF

Suggested Procedures

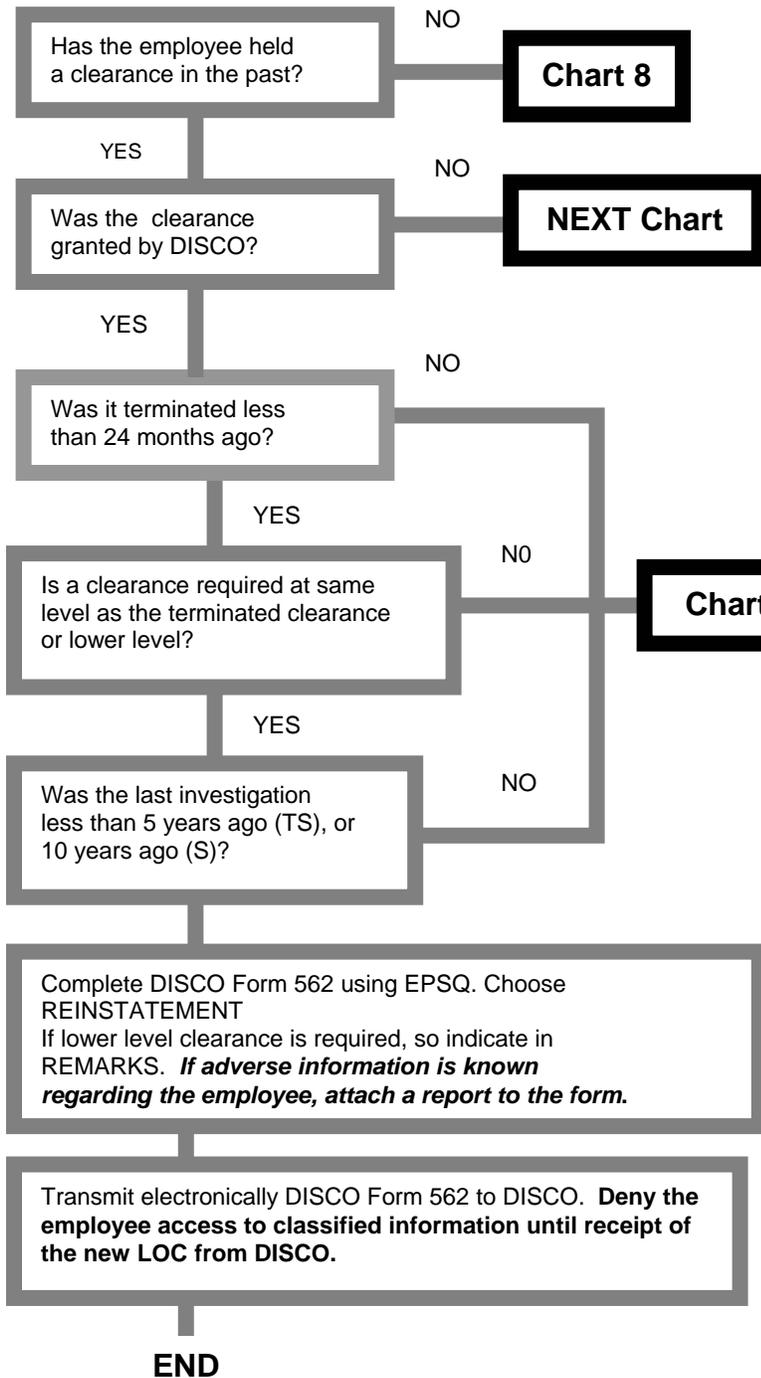


NOTE: Original SF 312s should be sent to DISCO on all new clearances. If, however, the losing facility has the original SF 312 for the transferring employee, it should be sent to DISCO.

Chart 6



Clearance Reinstatement



IMMIGRANT ALIEN LAA

Upon completion of the last contract for which access was authorized, you are required to terminate the LAA by transmitting Form 562 to DISCO. If access is necessary under a new contract, transmit a SF 86 to DISCO along with the UA endorsement (see chart 3). **Deny the employee access until receipt of a new LOC from DISCO.**

INVESTIGATIVE SCOPE

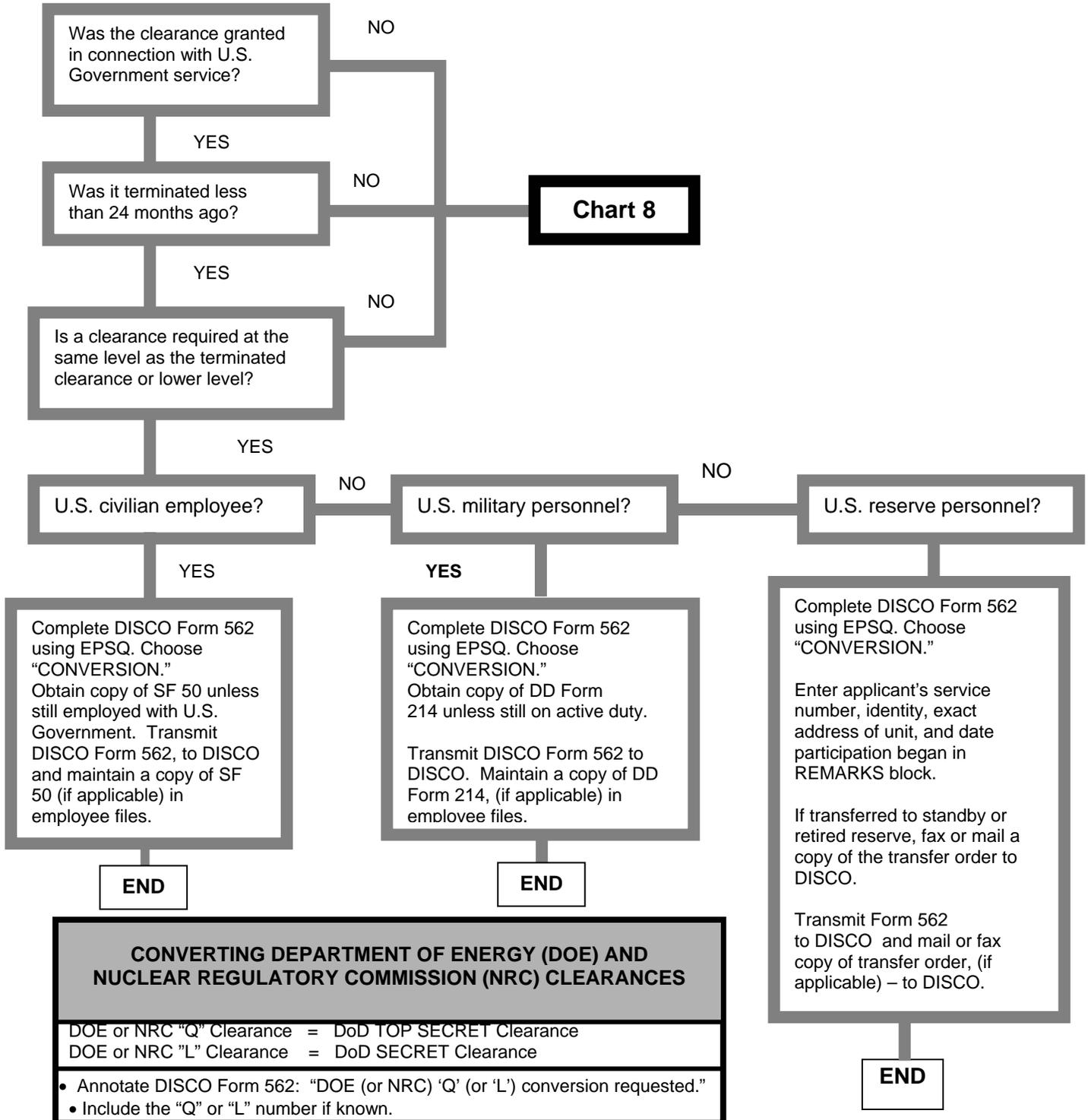
The last investigation must have met or exceeded the scope of the investigation required for the level of clearance that will be reinstated ---Single Scope Background Investigation (SSBI) for TOP SECRET clearances, or National Agency Check and Local Agency and Credit Check (NACLIC) for SECRET clearances.

Chart 7



Clearance Conversion

Employee holds or has held a clearance with a government activity.



CONVERTING DEPARTMENT OF ENERGY (DOE) AND NUCLEAR REGULATORY COMMISSION (NRC) CLEARANCES

DOE or NRC "Q" Clearance = DoD TOP SECRET Clearance
 DOE or NRC "L" Clearance = DoD SECRET Clearance

- Annotate DISCO Form 562: "DOE (or NRC) 'Q' (or 'L') conversion requested."
- Include the "Q" or "L" number if known.

Chart 8

<p>Employee required TOP SECRET Level PCL.</p>	<p>N E X T P A G E Chart 9</p>
<p>Employee is a non-U.S. citizen being processed for a SECRET or CONFIDENTIAL LAA.</p>	
<p>Employee required SECRET level PCL.</p>	<p>Chart 10</p>
<p>Employee requires CONFIDENTIAL level PCL.</p>	

Chart 9

STEP	TOP SECRET Clearance Processing
1	Fingerprint procedure. See Chart 11.
2	FSO completes DD form 1879. Choose, "Single Scope Background Investigation (SSBI)."
3	Complete SF 86 jointly with the employee. Brief employee about privacy option for Modules 17-42 of SF 86 using EPSQ. While it is optional, if employee completes those modules in private, the FSO can still validate and transmit the SF 86.
4	Review all viewable materials (DD Form 1879, SF 86 modules, and FD Form 258) for proper completion.
5	Transmit SF 86 electronically to DISCO and mail one signed FD Form 258 (fingerprint card) and the authority for release of information and records to DSS, Personnel Investigations Center/PIC 601 10th Street, Suite 125, Fort George Meade, MD 20755-5143. The authority for release of Information & Records may also be faxed to the Personnel Investigations Center (PIC), Tel: . 1-888-369-2812.
6	Refer to article 5, Industrial Security Letter (ISL) 02L-1, dated 22 Apr 02. When the SF 86 is submitted to DISCO electronically, the contractor/FSO is required to retain an original, signed copy of the SF 86 and authority for release of information and records until the clearance process has been completed.

END

Using the Electronic Personnel Security Questionnaire (EPSQ)
Complete guidance regarding how to use EPSQ is available at
www.dss.mil/EPSQ

Chart 10

STEP	SECRET/CONFIDENTIAL Clearance Processing
1	Fingerprint procedure. See Chart 11.
2	FSO completes NAC Security Information Sheet (equivalent to Part 1, Questions A through P of paper SF 86).
3	Complete SF 86 jointly with the employee. Brief employee about privacy option for modules 17-42 of SF 86 using EPSQ. While it is optional, if employee completes those modules in private, the FSO can still validate and transmit the SF 86.
4	Review FD Form 258 and all viewable pages of the SF 86 for proper completion.
5	Transmit SF 86 electronically to DISCO and mail one signed FD Form 258 (fingerprint card) and the authority for release of information and records to DSS, Personnel Investigations Center/PIC 601 10th Street, Suite 125, Fort George Meade, MD 20755-5143. The authority for release of Information & Records may also be faxed to the Personnel Investigations Center (PIC); Tel: 1-888-369-2812.
6	Refer to article 5, Industrial Security Letter (ISL) 02L-1, dated 22 Apr 02. When the SF 86 is submitted to DISCO electronically, the contractor/FSO is required to retain an original, signed copy of the SF 86 and authority for release of information and records until the clearance process has been completed.

END

**Using the Electronic Personnel Security Questionnaire
(EPSQ)**

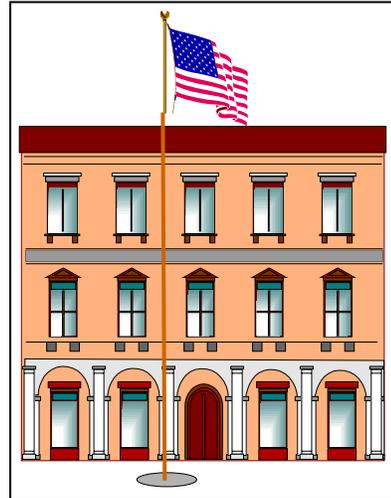
**Expert help is available regarding the EPSQ at
1-800-542-0237**

Chart 11

Fingerprinting Of Personnel Security Clearance Applicants

Use only those fingerprint cards printed in blue ink obtained from DISCO (FD 258).

Fingerprints may be taken at one of these places:



- At your facility
- be sure to review fingerprint cards in accordance with instructions on reverse of card

At the local police or sheriff's office

(Fee may be charged).

- Always send in at least one card to:

Mail: Defense Security Service
Personnel Investigations Ctr (PIC)
601 10th Street, Suite 125
Ft. George Meade, MD 20755-5134

When using an outside agency, send along another company employee as witness:



To verify identity of person being fingerprinted.



When using an outside agency the **witness** must return the fingerprint card(s) to the FSO to prevent substitution.

Chart 12

To double check your work, you can use the checklist below to make sure all major areas of concern have been covered.



CLEARANCE PROCESSING CHECKLIST

Step 1	Ascertain need for PCL. Chart 1 (p. 5-4)
Step 2	Determine that employee meets general requirements for PCL. Chart 1 & 2 (pp. 5-4 & 5-5)
Step 3	Determine which clearance procedure is called for, based on the employees current status and level of PCL required. Charts 3-8. (pp. 5-6 to 5-11)
Step 4	Complete appropriate forms. Charts 9-11 (pp. 5-12 to 5-14)
Step 5	Submit forms to DISCO.* Charts 9 & 10 (pp. 5-12 & 5-13)

***NOTE:** *DISCO encourages submission of EPSQ by electronic transmission.*

EPSQ software will be replaced by new E-QIP software sometime in 2004.

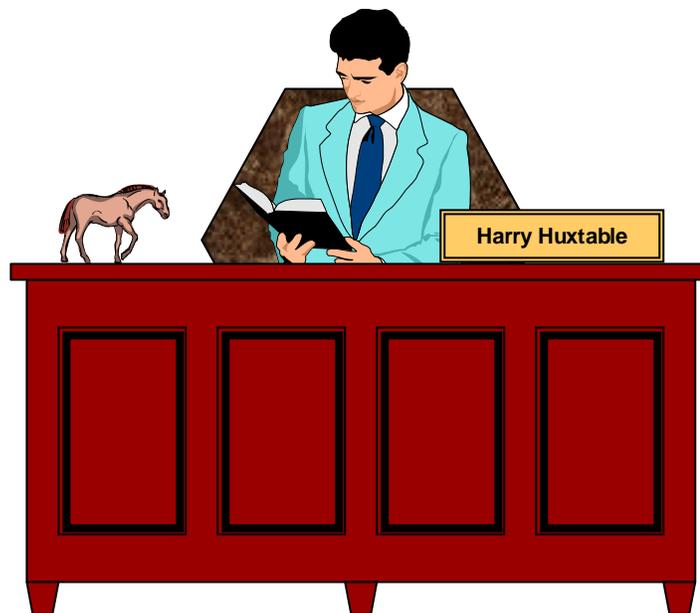
Information about OPM's E-QIP software is available at
www.opm.gov/e-qip

EXAMPLES OF PERSONNEL SECURITY CLEARANCE PROCEDURES

On the following pages we have provided some examples of the types of situations that can arise with personnel in need of PCLs.

In order to walk you through some of the possible situations, we have gone to our Home Office Facility, Electric Widget Company, for our examples. EWC is a much more complex operation than Electric Widget Services. EWC has a higher level Facility Security Clearance and on-site dealings with classified information.

For our review exercises at the close of this lesson we will, return to EWS for examples.



**Harold Huxtable. FSO for the
Electric Widget Company**

GENERAL GUNN METTLE

General Mettle retired almost a year ago from the US Army. The Electric Widget Company has hired the general and would like to use him on its TOP SECRET advanced widget program. Let's look at the process that Harold Huxtable, EWC's FSO, uses to determine what forms to have General Mettle fill out .



General Gunn Mettle, Ret.

NOTE: When using EPSQ for the conversion of PCL's it is not necessary to submit a copy of the DD 214 or SF 50 to DISCO. However, it is important that you maintain a copy in the employee file until the investigation is complete, in case there are any questions.

First, the PCL is warranted. There is a valid need for the general's clearance at the level requested. The project is classified TOP SECRET, and the material that the general would have to deal with in fulfilling his duties is TOP SECRET.

Since the request for a TOP SECRET level PCL is justified, Harold skips over to Chart 2 of the guide.

General Mettle is a US citizen. He has no relatives in any foreign country. He will not be a Key Management Person (KMP) in the company, so Harold continues on to Chart 7 , where the first block asks was the clearance granted in connection with U.S. Government Service?

The answer being "yes," Harold continues to follow Chart 7 on page 5-10. General Mettle's clearance was

granted in connection with his US Government service, so Harold moves down to the next block. Yes, General Mettle's clearance was terminated less than 24 months ago (10 months ago, to be exact), so Harold again moves down the "yes" path. General Mettle's clearance was at the TOP SECRET level, and this is the level of clearance he requires at EWC.

General Mettle was not a US civilian employee, so Harold takes the "no" path to "US military personnel." General Mettle, having been in the military, must follow the procedures under that heading. This involves the completion of a DISCO Form 562 and obtaining a copy of General Mettle's DD Form 214.

Harold then transmits the DISCO Form 562 to DSS and files the copy of the DD 214. And that takes care of the personnel security clearance application for General Gunn Mettle.



ROWENA OWENSBY, Ph.D.

ROWENA OWENSBY, Ph.D.

Dr. Owensby is one of Canada's leading laser physicists. EWC would very much like to employ her on the laser widget program. Mr. Wilbersnoot, EWC's president, asks Harold if this would be possible and, if so, how they should go about getting Dr. Owensby cleared. Harold explains to Mr. Wilbersnoot that they would first have to hire Dr. Owensby and *then* put in for her clearance. Mr. Wilbersnoot asks Harold to give him some idea of Dr. Owensby's chances for receiving a clearance if she were hired.

Harold, looking at the charts, follows the "yes" arrows down to Chart 2. Here he comes to the first "no" condition: Dr. Owensby is not a US citizen. Taking the path of the "no" arrow leads to Chart 3, where the first part of the question asks whether she has rare qualifications urgently needed for a specific classified contract. She does indeed. The second part of the question asks whether there is a suitable US citizen readily available for the job. To find out, Harold calls the

GCA for the laser widget program. He learns that, yes, there are several suitable US laser physicists in the greater Corinth area, two of whom are appropriately cleared and readily available. So the answer to the second part of the question is "no," directing Harold to stop the inquiry.

Harold goes back to Mr. Wilbersnoot with the bad news that using Dr. Owensby on the laser widget program would not be possible.

MILO MERTZ



MILO MERTZ

Milo has been working as a mailroom clerk at the Electric Widget Company this summer. His supervisor is so impressed with Milo that he would like to promote him to a better paying job. This job would involve the handling of CONFIDENTIAL material. The supervisor comes to Harold to see if this promotion is possible. He tells Harold he has never seen a more highly motivated or hard-working 16-year-old.

Reading down the first page of the charts, Harold answers the questions affirmatively. The clearance is needed and at the level requested (CONFIDENTIAL).

He is directed from Chart 2 to Chart 4 and, since Milo is not holding a current clearance granted by DISCO, Harold goes to Chart 6. Since Milo has not held a clearance in the past, Harold jumps to chart 8 and from there to Chart 10, where the details of preparing the application for Milo's CONFIDENTIAL clearance are spelled out. He gets back to the supervisor with the good news that Milo can, indeed, be promoted.

EVERY IVORY



EVERY IVORY

Mr. Ivory has been designing widgets for EWC since it was first organized. Last year he decided it was time to retire to his cabin in Kalispel, Montana. After only four months in the woods, however, he found himself longing for the feel of a newly manufactured widget in his hands. He renounced the big sky country and returned to Corinth, New York, to ask for his old job back. Mr. Wilbersnoot was delighted and told Harold to get Mr. Ivory cleared right away.

Harold knows from checking the records that Mr. Ivory meets all of the general requirements.

Following the chart on page 5-4, he is directed to Chart 4. The first block asks whether or not the employee is currently holding a DISCO-granted clearance. Mr. Ivory is not.

Harold turns to Chart 6. Mr. Ivory has held a TOP SECRET PCL at EWC within the last 24 months, so Harold reads down to the last block, where he discovers that to reinstate Mr. Ivory's clearance, Harold will need to submit a DISCO Form 562. (DISCO will issue a new LOC for Mr. Ivory, and Harold will ensure that he is **denied access** to classified information until the electronic LOC arrives.)

Harold and Mr. Ivory complete the DISCO Form 562, and Harold transmits it, using EPSQ pleasing Mr. Wilbersnoot to no end.

REVIEWING FORMS

Be sure to review all forms for accuracy, completeness, and continuity with any other forms being submitted. You and the employee complete the SF 86 *jointly*. Remember to:

- Advise the employee that he or she may complete modules 17-42 of the SF 86 in private. The EPSQ software has a “masking” feature that allows the employee to use this option. If the paper SF 86 is used, detach part 2 and advise the employee to seal it in an envelope, and give the envelope and the other completed pages of the form to you. Staple these two portions together before mailing them to DISCO.
- ***Employees are urged to use the computerized version of the SF 86. Use of the EPSQ automatically eliminates most of the errors common to completed typed-entry forms. Paper submissions will cause significant delays in the processing of a PCL.***

EPSQ Hints and Tips

* EPSQ requires middle names to successfully validate. If subject does not know a middle name, enter UNK in the middle name field

* EPSQ users can navigate more easily in modules where multiple entries are listed. To move more quickly, you can click:

- F7 to add a New Entry
- F8 to go back to the Previous Entry
- F9 to go to the Next Entry
- F10 to go to the Previous Module
- F11 to go to the Next Module

*If you don't know a zip code, they can be easily found at www.usps.gov/lookups.htm. This is a website for the US Postal Service.

There are over 50 Frequently Asked Questions (FAQs) at the EPSQ webpage at www.dss.mil/epsq. Information about E-QIP is available @ www.opm.gov/e-qip.

COMPLETED SAMPLES OF FORMS

The following pages contain examples of EPSQ submissions.

DoD REQUEST FOR PERSONNEL SECURITY INVESTIGATION DD Form 1879

This is the form you use to request a TOP SECRET personnel security investigation and a Periodic Reinvestigation (TOP SECRET). It is also used to request a SECRET or CONFIDENTIAL LAA.

Probably the best rule on when to use the DD Form 1879 is to use it for any clearance action other than a SECRET or CONFIDENTIAL clearance.

The DD Form 1879 always requires an accompanying SF 86.

When using EPSQ, if the applicant chooses SSBI or Periodic Reinvestigation as the type of investigation, EPSQ defaults to the DD 1879 for security information. When the Subject chooses NAC or Secret PR, EPSQ defaults to the NAC Security Sheet. The NAC Security Sheet is the equivalent of Part 1, A-P, of the paper SF 86.

When using EPSQ to apply for an LAA (Limited Access Authorization) you must contact the DISCO International Team and obtain a dummy social security number by calling 614-692-2136 or e-mail: occ_intl@mail.dss.mil. REMEMBER that the application will be returned without action if the original government justification is not submitted to DISCO. DISCO will accept a fax to begin the LAA process but must have the **original document** to complete the investigation. The fax number for LAA justification letters is 614-827-1651. The mailing address for the original documentation is:

DISCO
Attn: International Team
2780 Airport Drive
Suite 400
Columbus, OH 43219-2268

Initial screen seen by Security Officer when filling out DD1879 in EPSQ.

EPSQ

Create Modify Validation Reports Communications Utilities Help Exit

Navigation

1. Addresses (DD1879)
Request Personnel Investigation - 'From' Address
999-00-0001 BENNETT, ANTHONY YIP

Organization Code 346346

Organization Code Type CAGE Commercial and Government Entity Code

Requestor File No. (opt.) Request Date 1999/08/22

Do you require advance notice of NAC results? (Y/N) N No

Request Organization COACH CLASS CORP.

Address Line 1 12 CONTRACTOR DRIVE

Address Line 2

City BORING

State MD Maryland

Country/Zip or FPC UNITED STATES 21234

Next

Previous

Delete

Remarks

Help

Exit

Enter 1st line of address of the organization requesting this investigation

QUESTIONNAIRE FOR NATIONAL SECURITY POSITIONS - SF 86

This is the form used to apply for access to classified information.

Before submitting a SF 86, be sure that the FSO reviews it for justification.

Be sure to validate the forms and make corrections as necessary.

The package you submit to DISCO should include:

For TOP SECRET clearances, SECRET and CONFIDENTIAL LAAs, and other actions requiring a Single Scope Background Investigation (SSBI):

- DD Form 1879
- SF 86
- FD Form 258, "Fingerprint Card" (1 signed card*)

For SECRET and CONFIDENTIAL clearances:

- SF 86
- NAC Security Sheet (in EPSQ only)
- FD Form 258, "Fingerprint Card" (1 signed card)

Fingerprint cards are required for initial clearance requests.

***NOTE:** Request advice from DISCO on the number of fingerprint cards required to process an LAA. (The number depends on the country involved.)

Initial screen seen by applicant when filling out SF 86 in EPSQ.

Navigation

1. Personal Information (SF86)

999-00-0001 BENNETT, ANTHONY YIP

First Name	Middle	Last	Suffix
ANTHONY	YIP	BENNETT	

Birth Date 1920/12/16

City PASSAIC

State NJ New Jersey

County PASSAIC

Country UNITED STATES

Sex M Male

Next

Previous

Delete

Remarks

Help

Exit

Enter your first name

Initial screen seen by Security Officer when filling out NAC Security sheet in EPSQ.

EPSQ

Create Modify Validation Reports Communications Utilities Help Exit

Navigation

1. Addresses (NAC)

Forward This Request To...

900-62-0200 CHAINS, NEIL ANDREW

Name: DSS

Address Line 1: PERSONNEL INVESTIGATIONS CENTER

Address Line 2: P. O. BOX 28989

City: BALTIMORE

State/Zip: MD, Maryland 21240-8989

Next

Previous

Delete

Remarks

Help

Exit

Enter the name of the organization where you should send this request

When requesting a SECRET or CONFIDENTIAL clearance, using EPSQ, the FSO must complete the NAC Security Sheet (replaces Part 1, A-P on the paper SF 86).

PERSONNEL SECURITY CLEARANCE CHANGE NOTIFICATION - DISCO Form 562

When you report an employment termination use of the EPSQ is strongly recommended. **(See Chart 13, Page 5-30)**

A. CONCURRENT. A concurrent clearance applies when the employee already is a DISCO-cleared employee with another cleared contractor and requires a clearance at the same or lower level with your firm. ***The employee shall not have access until the LOC is issued.***

B. CONVERSION. Conversion applies when the person works or previously worked as a cleared employee for the Department of Defense, US military or another federal agency, such as the DOE or NRC. If the clearance was based on equivalent investigative requirements, it can be converted to a DISCO-granted clearance while the other clearance is active or within 24 months of the termination of the clearance. Note the following are DISCO equivalents of clearances issued by the Department of Energy (DOE) and the Nuclear Regulatory Commission (NRC):

- "Q" Clearance = TOP SECRET
- "L" Clearance = SECRET

Obtain a copy of DD Form 214 (if applicant is a former U.S military member) or a copy of SF 50 (if applicant was a US civilian employee). When using EPSQ, the DD 214 or SF 50 need not be sent to DISCO. However, maintain a copy in the employees file until the LOC is issued.

C. REINSTATEMENT. Reinstatement applies when the employee has no clearance, but has had a DISCO-granted clearance within the past 24 months and now requires a clearance at the same or lower level. The last investigation for clearance must have been completed not more than 5 years ago (TS) or 10 years ago (S). The last investigation must have met or exceeded the scope of the investigation required for the level of clearance that is to be reinstated— Single Scope Background Investigation (SSBI) for TOP SECRET clearance, or National Agency Check, Local Agency Check and Credit Check (NACLC) for SECRET clearance. If there is evidence of adverse information regarding the employee, attach a report of the information to the form.

D. MULTIPLE FACILITY TRANSFER. [Only when all PCLs **not** issued to HOF]

In REMARKS, enter:

- name, address and CAGE code of the facility to which the person is to be transferred.
- name and address of the submitting facility if different from information entered for name, address and zip code of employer.

I. DOWNGRADE. In REMARKS, enter "Downgrade without prejudice to (SECRET or CONFIDENTIAL)." To restore the former clearance level when needed, submit a new 562; mark **OTHER** block, and in REMARKS, enter "Upgrade to (TOP SECRET or SECRET)."

L. NAME CHANGE.

- In NAME OF EMPLOYEE, enter the person's former name exactly as shown on the LOC (or the SF 86 if the person is being processed for a clearance).

If all LOCs are issued to HOF/PMF:

- In REMARKS, enter name and address of the receiving HOF or PMF.

Initial screen seen by Security Officer when filling out DISCO Form 562 in EPSQ.

EPSQ

Create Modify Validation Reports Communications Utilities Help Exit

Navigation

1. Type of Action (DISCO562)

353-46-6554 TRUAX, THOMAS REGINALD Entry 1 of 1

Action Type **P Conversion** ▾

Enter the reason why you are preparing this form

[Next](#)

[Previous](#)

[Delete](#)

[Remarks](#)

[Help](#)

[Exit](#)

Chart 13

Clearance Termination

When is a PCL terminated?

Upon termination of employment
or
when the need for access to classified information presently or in the future is reasonably foreclosed.

How is a PCL terminated?

1. Complete DISCO Form 562.
2. Debrief employee. If the employee is a KMP, have him or her formally excluded from access to classified information via the board of directors meeting.
3. Submit DISCO Form 562 electronically. For KMP, also send a letter report, Change in KMPs along with a copy of the minutes of the board meeting at which the KMP was excluded from access to the DSS Field Office.

Can a terminated PCL be reactivated?

Reinstatement of a Terminated PCL

Terminated PCLs may be reinstated within 24 months when there is no known adverse information regarding the individual, the last investigation was not more than 5 years ago (TS) or 10 years ago (S), and the last investigation meets or exceeds the scope of the investigation required for the level of the PCL that is to be reinstated. Single Scope Background Investigation (SSBI) for TS or National Agency Check, Local Agency Check and Credit Check (NACLC) for S. To have the PCL reinstated, complete DISCO Form 562. Choose REINSTATEMENT. If adverse information is known regarding the individual, submit a report of the information to DISCO. Transmit the DISCO Form 562 to DISCO. **Deny the employee access until receipt of a new LOC.**

Procedures for Immigrant Alien LAA

Upon completion of the last contract for which access was authorized, terminate the LAA for the immigrant alien by submitting a DISCO Form 562 to DSS. If access is necessary under a new contract, submit an SF 86 to DSS along with the endorsement of the pertinent User Agency GCA (see chart 3). Deny the employee access until receipt of a new LOC from DISCO.

SAMPLE OF COMPLETED NAC SECURITY INFORMATION SHEET

SAMPLE OF COMPLETED NAC SECURITY INFORMATION SHEET

National Agency Check Security Information

Date: 1999/10/19

CHAINS

NEIL, ANDREW

EPSQ Version 2.1

Time: 14:34:14

SSN: 900-62-0200

Page: 1

1. Addresses

Forward This Request To:

DSS

PERSONNEL INVESTIGATIONS CENTER

P. O. BOX 28989

BALTIMORE, MD 21240-8989

RETURN RESULTS TO:

DISCO

2780 Airport Drive, Suite 400

Columbus, OH 43219-2268

Requester

Organization Code/Type E4T4TRG//CAGE

FROM:

DSS

244

ELKRIDGE LANDING RD

LINTHICUM, MD 21234

2. Type of Investigation

NAC - Industrial (3)

3. Local Files Check

YES Were the results of local files check favorable?

4. Current Status

What is the subject's current status? Consultant

5. Citizenship Verified

YES Was the subject's U.S. citizenship verified?

6. Reason for Request

Secret

Other

Remarks: Special project code r44445456

7. Investigation Validity Certification I certify that the information provided on this form is true to the best of my knowledge and that the above named individual has -he need for the indicated clearance to perform assigned duties.

Name of Certifier CASE
JUSTIN, LOUIS

Title of Certifier SECURITY MANAGER
Certifier's Phone 390490D

Certifier's Signature

Date

CERTIFICATION NOTICE

JUSTIN LOUIS CASE, SECURITY MANAGER, DSS, 244, ELKRIDGE LANDING RD, LINTHICUM, MD 21234 has certified to the Defense Security Service that NEIL ANDREW CHAINS has signed an Authority for Release of Information and Records authorizing any duly accredited representative of the Department of Defense (including those from the Defense Security Service) to obtain information relating to his/her activities. This Authority for Release of Information and Records will be maintained by DS3 until the security determination process has been completed.

An exact copy of the text of this Authority for Release of Information and Records, including all information provided on the form by NEIL ANDREW CHAINS (to include the name(s), date of birth, social security number, current home address, home telephone number, name signed on the release form, and date the release form was signed), is provided as an attachment to this notice and may be retained by the records repository or individual providing information concerning NEIL ANDREW CHAINS.

SAMPLE OF COMPLETED DISCO FORM 562 CLEARANCE CHANGE NOTIFICATION

EPSQ Version 2.1
O.M.B. No. 0704-0275
Time: 12:48:41

TRUAX

SSN: 353-46-6554

THOMAS, REGINALD

Page: 1

1. Type of Action

1. **Type of Change** P - Conversion
Separation Date 2003/05/30
Verifying Agency DEPARTMENT OF THE ARMY
PENTAGON
WASHINGTON, DC 20220

Did the subject receive an honorable discharge? Yes
NO Do you need to attach a DD214/SF50?

2. Personal Information

Name TRUAX
THOMAS, REGINALD
Maiden Name ****

DOB 1977/04/30 **POB** IRVINGTON, NJ
County ESSEX
Current Status
Citizenship UNITED STATES

3. Other Names

NO Was this subject known by any other names?

4. Employer Information

POLITENESS INC
244 ELKRIDGE LANDING RD
LINTHICUM, MD 21234
Phone Number 410 555 1333 **Cage Code** X4V345

5. Clearance Information

Level of Clearance Requested Top Secret
Current Clearance Information Top Secret
Date of Current Clearance 2001/11/08
Cleared By US ARMY

6. General Remarks

NO Do you have any remarks to enter regarding this change form?

7. Security Officer Information

I certify that the entries made above are true, complete, and correct to the best of my knowledge and belief.

Security Officer Name JACKSON
SAMUEL, V
Signature Date 2003/10/19

Security Officer's Signature

Date

SAMPLE OF COMPLETED SF 86 IN EPSQ

Office of Personnel Management
SECURITY CLEARANCE APPLICATION
Date: 1999/10/19
Standard Form 86, Sep. 95

EPSQ Version 2.1
O.M.B. No. 3206-0007
Time: 10:52:27

BENNETT
ANTHONY, YIP

SSN: 999-00-0001
Page: 1

1. Personal Information

Name BENNETT
ANTHONY, YIP

Birth Date 1920/12/16 Sex Male

Place Of Birth PASSAIC, NJ

County PASSAIC
UNITED STATES

Work/Day Phone 937-290-0880 Home/Evening Phone 937-372-0529

Height 5-11 Weight 219 Hair Color GRAY Eye Color BLUE

2. Other Names Used

YES Have you ever used or been known by another name?

FROM	TO	OTHER NAME
1. 1920/12/16	PRES	BENNETT TONY, YIP

3. Citizenship

Current Citizenship U.S. Citizen

Mother's Maiden Name GOOCH
MARY, GUIDA

Citizenship Type Born in the U.S.

NO Are you now or were you a dual citizen of the U.S. and another country?

4. Where You Have Lived

FROM	TO	ADDRESS
1. 1988/11/12	PRES	4 PALAMINO WAY FREDERICK, MD 21234

Person Who Knows You

NEWTON
WAYNE, FIG
7
PALAMINO WAY
LAS VEGAS, NV 89070
Phone 816-954-4952

NO Is this residence address hard to find?

5. Where You Went To School

NO Have you attended school beyond Junior High School within the last 10 years?
YES Have you attended school beyond high school? (If all education occurred more than 10 years ago, list most recent education beyond high school regardless of date.)

FROM	TO	TYPE/ADDRESS
1. 1988/10/20	1989/10/18	College/University/Military College
		Degree/Diploma/Other WIGGINS COLLEGE
		BA COLLEGE LANE
	Award Date 2000/01/19	YORK, PA 17791

6. Your Employment Activities

FROM	TO	TYPE OF EMPLOYMENT
1998/01/01	PRES	Federal Contractor

Your Position/Title

Employer Name LYTE INC
Employer Phone 410 929 2929
Job Address 22 W. 58TH STREET
TOWSON, MD 89907
Supervisor's Name YERBY

6. Your Employment Activities (Continued)

EDGAR, T

Supervisor Phone 410 992 2211

NO Is the employer's address different from the job location address?

NoAns Is the supervisor's address different from the job location address?

2. 1994/02/23 1998/01/23 Other Federal Employment

Your Position/Title HEAD WAITER

Employer Name HEADACHES DEPT

Employer Phone 409438543

Job Address 12 E WATER STREET
BALTIMORE, MD 21234

Supervisor's Name LAMP
TOM, K

Supervisor Phone 47746

NO Is the employer's address different from the job location address?

NO Is the supervisor's address different from the job location address?

NO Were you in the Federal Civil Service prior to the last 10 years?

7. People Who Know You Well

FROM	TO	REFERENCE NAME/ADDRESS
1. 1984/10/04	PRES	REDDING VERN, QUINCY Home Address 45 TREEHOUSE WAY TOLEDO, OH 43260 Evening Phone 445-548-5444
2. 1990/11/13	PRES	RD-FE DONNY, Q Home Address 12322 RAT ROAD NIKE, RI 04345 Day Phone 547-708-7866
3. 1982/10/13	PRES	EAST WALLY, W Work Address 632 JAZZ LANE NEW ORLEANS, LA 65340 Day Phone 434 434 4344

8. Your Spouse

What is your current marital status? Never Married

9. Your Relatives and Associates

RELATIONSHIP	NAME/PLACE OF BIRTH
1. Mother	GOOCH MARY, GUIDA DOB 1902/12/13 POB UNITED STATES NO Is the family/associate you listed deceased? Current Address 33 BROWN STREET POCOMOKE, MD 21232 Country(ies) of Citizenship UNITED STATES
2. Father	BENNETT ALDO, YEDI DOB 1903/11/01 POB UNITED STATES NO Is the family/associate you listed deceased? Current Address 7 SURGERY ST

9. Your Relatives and Associates (Continued)

TAMPA, FL 39423
Country(ies) of Citizenship UNITED STATES

10. Citizenship of Your Relatives and Associates

RELATIONSHIP	NAME
--------------	------

11. Your Military History

NO Have you ever served in the military? (If yes, provide in chronological order your military history: begin with the most recent period and include Reserves, National Guard, Merchant Marines, and Foreign Military service.)

12. Your Foreign Activities - Property

NO Do you have any foreign property, business connections, or financial interests?

13. Your Foreign Activities - Employment

NO Are you now or have you ever been employed by or acted as a consultant for a foreign government, firm, or agency?

14. Your Foreign Activities - Contact with Foreign Government

NO Have you ever had any contact with a foreign government, its establishments (embassies or consulates), or its representatives, whether inside or outside the U.S., other than on official U.S. Government business? (Does not include routine visa applications and border crossing contacts.)

15. Your Foreign Activities - Passport

NO In the last 7 years, have you had an active passport that was issued by a foreign government?

16. Foreign Countries You Have Visited

NO Have you traveled outside the United States on other than official U.S. Government orders in the last 7 years? (Travel as a dependent or contractor must be listed.) Do not repeat travel covered in modules 4, 5, and 6.

17. Your Military Record

NO Have you ever received other than an honorable discharge from the military?

18. Your Selective Service Record

NO Are you a male born after December 31, 1959?

19. Your Medical Record

NO In the last 7 years, have you consulted a mental health professional (psychiatrist, psychologist, counselor, etc.) or have you consulted with another health care provider about a mental health related condition?

20. Your Employment Record

NO Has any of the following happened to you in the last 10 years?

- Fired from job
- Quit a job after being told you'd be fired
- Left a job by mutual agreement following allegations of misconduct
- Left a job by mutual agreement following allegations of

20. Your Employment Record (Continued)

unsatisfactory performance

- Left a job for other reason under unfavorable circumstances

21. Your Police Record - Felony Offenses

NO Have you ever been charged with or convicted of any felony offense?

(Include those under the Uniform Code of Military Justice.) For this item, report information regardless of whether the record in your case has been "sealed" or otherwise stricken from the record. The single exception to this requirement is for certain convictions under the Federal Controlled Substances Act for which the court issued an expungement order under the authority of 21 U.S.C. 844 or 18 U.S.C. 3607.

22. Your Police Record - Firearms/Explosives Offenses

NO Have you ever been charged with or convicted of a firearms or explosives offense? For this item, report information regardless of whether the record in your case has been "sealed" or otherwise stricken from the court record. The single exception to this requirement is for certain convictions under the Federal Controlled Substances Act for which the court issued an expungement order under the authority of 21 U.S.C. 844 or 18 U.S.C. 3607.

23. Your Police Record - Pending Charges

NO Are there currently any charges pending against you for any criminal offense? For this item, report information regardless of whether the record in your case has been "sealed" or otherwise stricken from the record. The single exception to this requirement is for certain convictions under the Federal Controlled Substances Act for which the court issued an expungement order under the authority of 21 U.S.C. 844 or 18 U.S.C. 3607.

24. Your Police Record - Alcohol/Drug Offenses

NO Have you ever been charged with or convicted of any offense(s) related to alcohol or drugs? For this item, report information regardless of whether the record in your case has been "sealed" or otherwise stricken from the record. The single exception to this requirement is for certain convictions under the Federal Controlled Substances Act for which the court issued an expungement order under the authority of 21 U.S.C. 844 or 18 U.S.C. 3607.

25. Your Police Record - Military Court

NO In the last 7 years, have you been subject to court martial or other disciplinary proceedings under the Uniform Code of Military Justice? (include non-judicial, Captain's mast, etc.) For this item, report information regardless of whether the record in your case has been "sealed" or otherwise stricken from the record. The single exception to this requirement is for certain convictions under the Federal Controlled Substances Act for which the court issued an expungement order under the authority of 21 U.S.C. 844 or 18 U.S.C. 3607.

26. Your Police Record - Other Offenses

NO In the last 7 years, have you been arrested for, charged with, or convicted of any offense(s) not listed in modules 21, 22, 23, 24, or 25? (Leave out traffic fines of less than \$150 unless the violation was alcohol or drug related.) For this item, report information regardless of whether the record in your case has been "sealed" or otherwise stricken from the record. The single exception to this requirement is for certain convictions under the Federal Controlled Substances Act for which the court

26. Your Police Record - Other Offenses (Continued)

issued an expungement order under the authority of 21 U.S.C. 844 or 18 U.S.C. 3607.

27. Your Use of Illegal Drugs and Drug Activity-Illegal Use of Drugs

NO Since the age of 16 or in the last 7 years, whichever is shorter, have you illegally used any controlled substance, for example, marijuana, cocaine, crack cocaine, hashish, narcotics (opium, morphine, codeine, heroin, etc.), amphetamines, depressants (barbiturates, methaqualone, tranquilizers, etc.), hallucinogenics (LSD, PCP, etc.), or prescription drugs?

28. Your Use of Illegal Drugs and Drug Activity-Use in Sensitive Positions

NO Have you EVER illegally used a controlled substance while employed as a law enforcement officer, prosecutor, or courtroom official; while possessing a security clearance; or while in a position directly and immediately affecting public safety?

29. Your Use of Illegal Drugs and Drug Activity-Drug Activity

NO In the last 7 years, have you been involved in the illegal purchase, manufacture, trafficking, production, transfer, shipping, receiving, or sale of any narcotic, depressant, stimulant, hallucinogen, or cannabis for your own intended profit or that of another?

30. Your Use of Alcohol

NO In the last 7 years has your use of alcoholic beverages (such as liquor, beer, wine) resulted in any alcohol-related treatment or counseling (such as for alcohol abuse or alcoholism)? Do not repeat information reported in module 21 on form SF86 (Your Medical Record).

31. Your Investigation Record - Investigations/Clearances Granted

NO Has the United States Government ever investigated your background and/or granted you a security clearance? (If you can't recall the investigating agency and/or the security clearance received, enter (Y)es and follow instructions in the help text for the fields on the next screen. If you can't recall whether you've been investigated or cleared, enter (N)o.)

32. Your Investigation Record - Clearance Actions

NO To your knowledge have you ever had a clearance or access authorization denied, suspended, or revoked, or have you ever been debarred from government employment? (Note: An administrative downgrade or termination a security clearance is not a revocation.)

33. Your Financial Record - Bankruptcy

NO In the last 7 years, have you filed a petition under any chapter of the bankruptcy code (to include Chapter 13)? of

34. Your Financial Record - Wage Garnishments

NO In the last 7 years, have you had your wages garnished for any reason?

35. Your Financial Record - Repossessions

NO In the last 7 years, have you had any property repossessed for any reason?

36. Your Financial Record - Tax Lien

NO In the last 7 years, have you had a lien placed against your property for failing to pay taxes or other debts?

37. Your Financial Record - Unpaid Judgements

YES In the last 7 years, have you had any judgements against you that have not been paid?

<u>DATE</u>	<u>AMOUNT/NAME ACTION OCCURRED UNDER</u>
1. 1994/05/22	709 RHANATIC PHIL, LEE

Court Name DISTRICT COURT
Address PHILADELPHIA, PA 17793

38. Your Financial Delinquencies - 180 Days

NO In the last 7 years, have you been over 180 days delinquent on any debt(s)?

39. Your Financial Delinquencies - 90 Days

NO Are you currently over 90 days delinquent on any debt(s)?

40. Public Record Civil Court Actions

NO In the last 7 years, have you been a party to any public record civil court actions not listed elsewhere on this form?

41. Your Association Record - Membership

NO Have you ever been an officer or a member or made a contribution to an organization dedicated to the violent overthrow of the United States Government and which engages in illegal activities to that end, knowing that the organization engages in such activities with the specific intent to further such activities?

42. Your Association Record - Activities

NO Have you ever knowingly engaged in any acts or activities designed to overthrow the United States Government by force?

43. General Remarks

NO Do you have any additional remarks to enter in your application?

CERTIFICATION BY PERSON COMPLETING FORM

My statements on this form, and any attachments to it, are true, complete, and correct to the best of my knowledge and belief and are made in good faith. I understand that a knowing and willful false statement on this form can be punished by fine or imprisonment or both. (See section 1001 of title 18, United States Code).

Name BENNETT
ANTHONY, YIP
SSN 999-00-0001

Signature (Sign in ink)

Date

UNITED STATES OF AMERICA

Authorization for Release of *Information*

Carefully read this authorization to release information about you, then sign and date it in ink.

I Authorize any investigator, special agent, or other duly accredited representative of the authorized Federal agency conducting my background *investigation*, to obtain any information relating to my activities from individuals, schools, residential management agents, employers, criminal justice agencies, credit bureaus, consumer reporting agencies, collection agencies, retail business establishments, or other sources of information. This information may include, but is not limited to, my academic, residential, achievement, performance, attendance, disciplinary, employment history, criminal history record *information*, and financial and credit *information*. I authorize the Federal agency conducting my investigation to disclose the record of my background investigation to the requesting agency for the purpose of making a determination of suitability or eligibility for a security clearance.

I Understand that, for financial or lending institutions, medical *institutions*, hospitals, health care professionals, and other sources of *information*, a separate specific release will be needed, and I may be contacted for such a release at a later date. Where a separate release is requested for information relating to mental health treatment or counseling, the release will contain a list of the specific questions, relevant to the job description, which the doctor or therapist will be asked.

I Further Authorize any investigator, special agent, or other duly accredited representative of the U.S. Office of Personnel Management, the Federal Bureau of Investigation, the Department of Defense, the Defense Investigative Service, and any other authorized Federal agency, to request criminal record *information* about me from criminal justice agencies for the purpose of determining my eligibility for access to classified *information* and/or for *assignment* to, or retention in, a sensitive National Security position, in accordance with 5 U.S.C. 9101. I understand that I may request a copy of such records as may be available to me under the law.

I Authorize custodians of records and other sources of *information pertaining* to me to release such *information* upon request of the investigator, special agent, or other duly accredited representative of any Federal agency authorized above regardless of any previous agreement to the contrary.

I Understand that the information released by records custodians and sources of information is for official use by the Federal Government only for the purposes provided in this Standard Form 86, and that it may be redisclosed by the Government only as authorized by law.

Copies of this authorization that show my signature are as valid as the original release signed by me. This authorization is valid for five (5) years from the date signed or upon the *termination* of my affiliation with the Federal Government, whichever is sooner. Read, sign, and date the release on the next page if you answered "Yes" to question 21.

Signature (Sign in ink) SSN 999-00-0001

Date

Name BENNETT
ANTHONY, YIP
Other **Names Used** BENNETT
TONY, YIP
Address 4 PALAMINO WAY

FREDERICK, MD 21234
SSN 999-00-0001 **Home**
Phone 937-372-0529

Standard Form 86
Revised September 1995
I.S. Office of Personnel Management
CFR Parts 731, 732, and 736

Form approved:
O.M.B. No. 3206-0007
NSN 7540-00-634-4036
86-111

UNITED STATES OF AMERICA
AUTHORIZATION FOR RELEASE OF MEDICAL INFORMATION

(Carefully read this authorization to release information about you, then sign and date it in ink.)

Instructions for Completing this Release

This is a release for the investigator to ask your health practitioner(s) the three questions below concerning your mental health consultations. Your signature will allow the practitioner(s) to answer only these questions.

I am seeking assignment to or retention in a position with the Federal government which requires access to classified national security information or special nuclear information or material. As part of the clearance process, I hereby authorize the investigator, special agent, or duly accredited representative of the authorized Federal agency *conducting* my background investigation, to obtain the following *information* relating to my mental health consultations:

Does the person under investigation have a condition or treatment that could impair his/her judgement or reliability, particularly in the context of safeguarding classified national security information or special nuclear information or material?

If so, please describe the nature of the condition and the extent and duration of the impairment or treatment.

What is the prognosis?

I understand the information released pursuant to this release is for use by the Federal Government only for purposes provided in the Standard Form 86 and that it may be redisclosed by the Government only as authorized by law.

Copies of this authorization that show my signature are as valid as the original release signed by me. This authorization is valid for 1 year from the date signed or upon termination of my affiliation with the Federal Government, whichever is sooner.

Signature (Sign in ink) SSN 999-00-0001 Date

Name BENNETT
ANTHONY, YIP
Other Names Used BENNETT
TONY, YIP
Address 4 PALAMINO WAY

FREDERICK, MD 21234
SSN 999-00-0001 **Home Phone**
937-372-0529

* ----- *

2. Request For . . . Information

Request Type: Single Scope Background Investigation (SSBI)

3. Application Status

Select the highest level of classified material to which the subject of the investigation will have access: Top Secret
TS Billet Number: 112124

4. Investigation Status Reason

for Access: OODEP

5. Citizenship Verification

YES Was the subject's U.S. citizenship verified?

Document: Birth certificate

6. Files Verification

FILE VERIFIED	DATE	FINDING (FAV, NAV, NOR, UNF)
PERSONNEL	1999/10/10	FAV
MEDICAL	1999/10/11	FAV
SECURITY	1999/10/12	FAV
BASE/MILITARY POLICE	1999/10/14	NAV
PRE SCREENING INTERVIEW	1999/10/16	FAV
EMPLOYMENT	1999/04/21	FAV

7. Prior Investigations

Select the highest level of classified material to which the subject of the investigation will have access: Top Secret

TYPE Top Secret **DATE** 19900321 **REQ FILE NUMBER** 1028
AGENCY DIS

8. Title or Position of Subject

Remarks: Head Deal Maker

9. List of Enclosures **Remarks:** None

10. Reason for Access to Classified Material

Remarks: Will be viewing classified contract documents.

11. History of Government/Military Employment

How would you characterize the accuracy of the Government Employment and/or Military Service History indicated by the subject's form? Correct

12. General Remarks

13. Investigation Validity Certification

I certify that the information provided on this form is true to the best of my knowledge and that the above named individual has the need for the indicated clearance to perform assigned duties.

Name of Certifier REDMAN
EDWARD, T
Title of Certifier CERTIFIER
Certifier's Phone 3467 64634

13. Investigation Validity Certification (Continued)
Certifier's Signature

Date

14. Supervisor's Certification

The immediate supervisor is NOT aware of adverse information concerning the individual named within this form.

Immediate Supervisor EDWARDS
ERIC, W
Supervisor Title SUPERVISOR
Supervisor's Phone 3467457
Signature Date 1999/04/11

Supervisor's Signature

Date

CERTIFICATION NOTICE

EDWARD T REDMAN , CERTIFIER, DSS, 244, ELKRIDGE LANDING RD, LINTHICUM, MD 21234 has certified to the Defense Investigative Service that ANTHONY YIP BENNETT has signed an Authority for Release of Information and Records authorizing any duly accredited representative of the Department of Defense (including those from the Defense Investigative Service) to obtain information relating to his/her activities. This Authority for Release of Information and Records will be maintained by DSS until the security determination process has been completed.

An exact copy of the text of this Authority for Release of Information and Records, including all information provided on the form by ANTHONY YIP BENNETT (to include the name(s), date of birth, social security number, current home address, home telephone number, name signed on the release form, and date the release form was signed), is provided as an attachment to this notice and may be retained by the records repository or individual providing information concerning ANTHONY YIP BENNETT .

Industry Customers Can Now Fax Releases to DSS

DSS is now able to accept faxed releases from Industrial customers concurrent with the submission of EPSQs. Faxing the general releases makes them immediately available to our field investigators and facilitates initial investigative work as soon as the case is opened. You may begin faxing releases immediately. While faxing the release is optional, we strongly encourage you to utilize the service. Please be assured that to protect privacy information, only authorized DSS personnel will receive and process faxed releases.

Procedural Instructions for Faxing Releases to DSS

- Releases should be faxed at the same time investigative requests are transmitted via EPSQ to DSS. The toll-free number to fax your release(s) is **1-888-369-2812**.
- It is extremely important to use *only* the coversheet provided with these instructions when faxing releases. Please *do not* create your own coversheet(s), modify the coversheet provided **OR** fax release(s) without a coversheet. The coversheet furnished will be directly utilized by our automated scanning system to process the releases and has already been tested and approved for compatibility.
- Ensure that all releases are signed and reflect a legible social security number.
- Ensure that all coversheets are completely annotated.
- Please send **one coversheet** per applicant. If you are faxing multiple releases related to one applicant, only use one coversheet (i.e., do not create a separate coversheet for each release related to the same Subject).
- When sending releases on multiple applicants at once, please ensure that all coversheets and releases are faxed in order. Doing so is important for accountability in the automation process at DSS.
- It is not necessary to contact DSS subsequent to faxing releases to ensure that they have been received. If there was a problem with the fax transmission (i.e., a garbled fax or page(s) missing), DSS personnel will call the point of contact indicated on the coversheet.

IMPORTANT: Please do not mail releases subsequent to faxing them. Doing so will create duplicate entries and slow the process down.

Company/Command Name: _____

Address: _____

RELEASE FAX COVER SHEET

Date: _____

SUBJECT: _____

SSN: _____

Comment:

Defense Security Service
Records Management Group
FAX: 1-866-369-2812

The following release(s) attached:

_____ General Release(s)

_____ Medical Release(s)

_____ Other

If the release(s) are not complete/legible or if there are transmission problems,
please contact:

Name _____

Phone/Cell Phone _____

This cover sheet is Page 1 of _____ pages.

WARNING

Information attached is U.S. Government Property. If you are not the intended recipient of this information, disclosure, reproduction, distribution, or use of this information is prohibited (18.U.S.C. 641). Please notify the originator or the local DSS Office immediately to arrange for proper disposition.

FOR OFFICIAL USE ONLY

SUMMARY

Based on the status of the applicant and on the level of access required, various forms and other documents are submitted to DISCO to apply for industrial personnel security clearances (PCLs) or limited access authorizations (LAAs). PCLs are granted by DISCO at the TOP SECRET, SECRET, or CONFIDENTIAL level to US citizens only. LAAs may be granted by DISCO at the SECRET or CONFIDENTIAL level to immigrant aliens and foreign nationals. Application for an initial TOP SECRET clearance is by submission of SF 86, DD Form 1879, and FD Form 258 (fingerprint card) to DISCO. These forms are also submitted for any level of clearance when the applicant is a representative of a foreign interest (RFI), or the applicant is an immigrant alien or foreign national (LAA applicant). Application for an initial SECRET or CONFIDENTIAL clearance is by submission of SF 86 and FD Form 258 to DISCO. FSOs must ensure that PCL or LAA applications are strictly limited to the minimum required for performance of the facility's classified contract(s).

FSOs and employees must use the EPSQ Version 2.2 software for all actions which require completion of the SF 86, DD Form 1879 and DISCO Form 562. This **free** software can be downloaded from the DSS website – www.dss.mil. EPSQ software will be replaced sometime in 2004 by E-QIP software. Information about E-QIP software is available at www.opm.gov/e-qip.

Besides initial clearance actions, the NISPOM provides for concurrent clearances, clearance transfers within a multiple-facility organization (MFO) when an alternative to issuing all clearances to the Home Office Facility (HOF) has been approved, clearance reinstatements, and clearance

conversions. All of these actions require the submission of DISCO Form 562 to DISCO.

The FSO should act to have clearances that are no longer required terminated by debriefing the employee and notifying DISCO of the action by sending a DISCO Form 562.

Introduction of the JPAS system in 2004 will significantly change the procedures presented in this lesson.

5 - Review Exercises

Complete the following exercises for review and practice.

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



Answer the first seven questions using the charts found in this lesson.

1. Roberta Baloon is cleared SECRET at EWS. She works as a service person on classified jobs at Air Force sites. Getting Roberta cleared was a relatively simple matter. She's a US citizen with no foreign connections and no problems of any kind in her background.

What forms did Harriet need to prepare for the clearance application?

2. When Wanda Fishtank was made the FSO at EWS, she only held the post for two weeks, she had to be cleared at the level of EWS's facility clearance.

What forms did she use?

3. Mr. Wilbersnoot has recommended Ozbak Pleebo, an immigrant alien from Freedonia, for a CONFIDENTIAL LAA. Ozbak is one of the few people in this country capable of doing extremely detailed repair work on a certain classified widget, and the others are unavailable to perform on the repair contract.

What should she do to obtain an LAA for Ozbak? _____

4. Jimbo Duggins left EWS for a try at freelance widget repair. This endeavor did not prove as profitable as he had hoped and he returned to the economic security of his old job before eight months had passed. He had held a SECRET clearance before leaving and required it again upon his return.

What form did Harriet submit to reinstate his clearance?_____.

5. Monica Zilla is a seventeen year old whiz kid who graduated last year from M.I.T. Gizmo Corporation wants her on their TOP SECRET research project.

Can she be an applicant for a TOP SECRET clearance? _____.

6. Jimbo Duggins, having returned to his old job at EWS, has an opportunity to earn additional income by working evenings as a security guard at Digital Widgets, Inc. (DWI). This second job also requires a SECRET security clearance.

What form has to be submitted to allow Jimbo to hold a concurrent clearance?_____.

7. Felicia Picklesby worked as a civilian for the Army, grade GS-9, until her retirement five months ago. Now she's going to work as a government contract specialist at Digital Widgets (DW). She was cleared SECRET during her entire government career and will require a SECRET clearance at DW.

What can be done to convert her prior clearance?_____

8. If you do not know someone's middle name leave it blank.

True False.

9. FD Form 258, Fingerprint Card, is submitted with SF 86 for an initial clearance.

True False.

10. The cause of the most significant delays in DISCO's processing of Personnel Security Questionnaires is:

- a. failure to submit fingerprint cards with application.
- b. failure of the applicant to complete the signature block.
- c. failure to use EPSQ
- d. illegible forms.

11. Duncan Undersides, a serviceman cleared SECRET at EWS, doesn't require his clearance any longer. He still works for EWS, but not on classified projects.

After Harriet has debriefed Duncan, what form does she use to notify DISCO of the termination of his security clearance?

12. Harriet may apply to have Duncan's clearance reinstated if he again requires it within _____ months.

13. Match the form(s) that are typically used in applying for the level of clearance indicated or in taking the clearance action described.

Clearance/Clearance Action	Form
_____ CONFIDENTIAL clearance	
_____ Transfer within a multiple facility organization *	a. SF 86
_____ SECRET Clearance	b. FD Form 258
_____ Conversion of a prior military clearance within 24 months	c. DISCO Form 562
_____ Reinstatement of a clearance that was terminated less than 24 months ago	d. SF 50
_____ TOP SECRET Clearance	e. DD Form 1879
_____ Concurrent Clearance	f. DD Form 214
_____ Clearance Termination	h. Electronic Letter of Consent
_____ Conversion of a prior civilian clearance within 24 months	

*When an alternative arrangement approved so that all PCLs are **not** issued to HOF.

14. What does the acronym JPAS stand for and what current administrative security actions will JPAS replace? _____

5- Solutions & References



1. Harriet transmitted the SF 86 using EPSQ and FD Form 258 (fingerprint card) for Roberta to PIC. (Charts 1, 2, 8, & 10) (Pgs. 5-4, 5-5, 5-11, & 5-13)
2. Since EWS's facility clearance is at the SECRET level, she transmitted the SF 86 using EPSQ and mailed the FD Form 258 to PIC. (pgs. 5-2 & 5-3) (Charts 1 & 10)
3. She must ensure that all requirements of 2-210, NISPOM are met. Then she should transmit the SF 86, DD Form 1879, mail the FD Form 258 to PIC, and mail the original User Agency (GCA) endorsement and any other supporting documentation to DISCO. (Pg 5-5 & 5-6) (Charts 2, & 3)
4. DISCO Form 562. (chart 6) (Pg. 5-9)
5. Yes, there is no minimum age requirement for a clearance. (charts 1,2,8 & 9) Pgs. 5-4,5-5, 5-11,5-12 & 5-19)
6. DISCO Form 562. (chart 4) (Pg. 5-7)
7. Transmit DISCO Form 562 to DSS maintain a copy of the SF 50. (Chart 7) (Pg. 5-10)
8. False. (Pg. 5-21)
9. True.(Charts 9 & 10) (Pgs. 5-12 & 13)
10. c. (Pg. 5-21)
11. Harriet will transmit a DISCO Form 562 to DSS. (chart 13 (Pg. 5-30)

12. 24. Should Duncan again need his clearance within 24 months of the termination, it can be reinstated using a DISCO Form 562, provided there is no adverse information. (Chart 6)

13. a, b CONFIDENTIAL clearance
 c, h Transfer within a multiple facility organization
 a, b, SECRET clearance
 c, f Conversion of military clearance
 c Reinstatement of a SECRET clearance
 a, b, e TOP SECRET clearance
 c Concurrent clearance
 c Clearance termination
 c, d Conversion of civilian clearance

(Charts, 1 & 7) Pages 5-4 & 5-10.

14. The acronym JPAS stands for, Joint Personnel Adjudication System. JPAS is the system of the future that will handle all transactions such as, terminations, PCL upgrades, downgrades, reinstatements and maintaining non-disclosure signature dates. JPAS will be used extensively by contractors participating in the National Industrial Security Program (NISP). (Page 5-1, and DoD ISL 02L-1, dated 22 April 2002)

LESSON 6

Reports

For the National Industrial Security Program to work, there must be communication between government and industry. On the government's part, this communication takes the form of directives and guidance, as well as security reviews to see that the program is working on site. On the part of industry, this communication largely takes the form of reports to the government. These reports are simply your way of letting DSS know what's going on. In a cooperative venture like the NISP, it's necessary that all parties be informed.

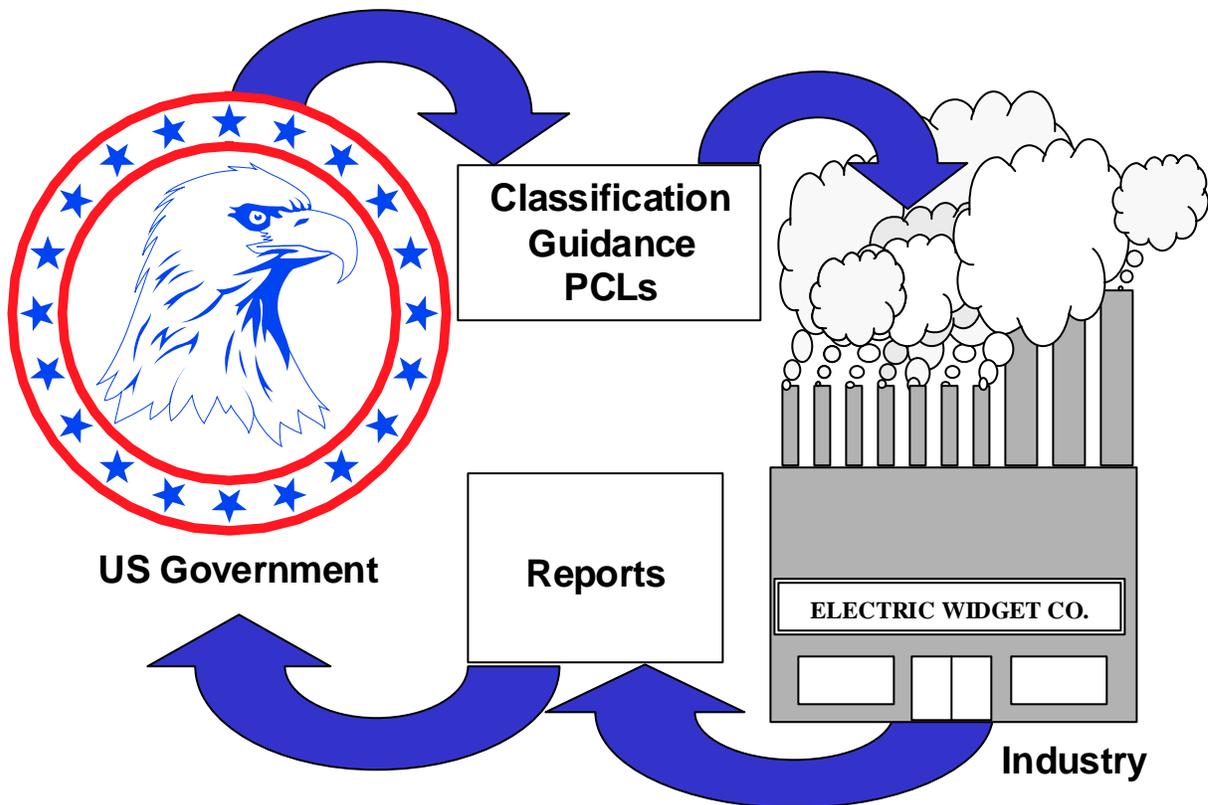
OBJECTIVES

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

- Describe the reporting requirements.
- Explain the definition of adverse information and where to send the report.
- Locate the proper reporting requirement, given a certain situation, and complete the appropriate reporting requirement.
- Differentiate between reports sent to the DSS Field Office or reports sent to DISCO.

REPORTING REQUIREMENTS UNDER THE NISP

One of your most important duties as an FSO is to make required reports to the government. These reports are a link in the government/industry relationship that we outlined in Lesson 1. While there are a number of specific reports required by the NISP, these reports generally fall into three categories. This should make it easier for you to determine when a report is warranted and to determine how to make that report.



The first category of reports concerns *changes*: **changes affecting cleared personnel** and **changes that affect the Facility Security Clearance**. If there is any change pertaining to your company's FCL or PCLs you should check paragraph 1-302 of the NISPOM to see if the changed condition requires that a report be sent. We will look at some examples of these reports and how to make them later in the lesson.

The second category is **adverse information** reporting. This report reflects a changed condition that affects an individual's personnel security clearance (PCL) which falls under the first category. We're treating adverse information reporting as a separate type of report because of its extreme importance to the National Industrial Security Program. This lesson provides a good opportunity to explain

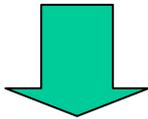
the philosophy of adverse information reporting, its purpose, and some of the legal implications of this report for industry.

The third reporting category concerns classified information directly. These are reports that are made when there is *loss, compromise, or suspected compromise* of classified information.

HOW THE NISPOM IS ARRANGED FOR REPORTING REQUIREMENTS



EMPLOYEES



FSO

DSS Field Office

DISCO

FBI

How reports get to the Government

Section 3 of the NISPOM divides the reports in terms of *where they are sent*. Reports regarding espionage, sabotage, or subversive activities are sent to the Federal Bureau of Investigation (FBI), as described in paragraph **1-301**. Reports sent to the Cognizant Security Agency (CSA) are listed in 1-302. Paragraphs 1-303 indicate reports sent to your DSS Representative. Paragraph 1-304 outlines reports that are sent to DISCO.

Much confusion stems from the use of the term "CSA" (a high-level term that refers to any one of the four major government players of the NISP). What the report writer needs to know are low-level terms that specify where to send the various reports. The high-level term is "CSA," which stands for "Cognizant Security Agency." The CSA is, the DOE, the NRC, the CIA, or the DoD, which ever is your CSA. DSS is a part of DoD.

Cognizant Security Office. The "CSA" also includes two elements of DSS: DISCO and your DSS Field Office. *You actually send the reports for the "CSA" to DISCO or your DSS Field Office.* Throughout this lesson, we'll point out which CSA reports go to which DSS element.

WHAT IS A REPORT?

A report may take a number of different forms. In some cases it is merely the act of notification, by letter or telephone, or e-mail that something has occurred. Other reports have more specific procedures such as use of a certain form or requirements for a detailed listing of information. Once you have determined what information needs to be reported, you can easily check the charts provided in this lesson for that reporting requirement and determine how it should be reported.

PEOPLE CHANGES AND FACILITY CHANGES

All 1-302 reports that reflect changes affecting *Personnel Security Clearances* are sent to DISCO. Most often you will use DISCO Form 562, (Personnel Security Clearance Change Notification), to make your reports to DISCO. DISCO Form 562 is the "CSA designated form" mentioned in 1-302c and 1-302e. It is used to report a name change, termination of employment, termination of clearance, etc. Otherwise, a letter report to DISCO is called for.

Example of a Changed Condition: Name change of a cleared employee.

BEFORE



Dr. Jekyll

AFTER



Mr. Hyde

NOTE: There could also be a potential adverse information report here.

All paragraph 1-302 reports that reflect changes regarding the *Facility Security Clearance* are sent, in writing, *to the DSS Field Office*. Most reports to the DSS Field Office will be made by letter. These are the 1-302h reports that we discussed in Lesson 3; those that advise the DSS Field Office of changed conditions that affect your FCL. You will recall that only one type of report to the DSS Field Office entails submitting a SF 328 report form: as discussed in paragraph 1-302h(5) of the NISPOM. This requirement to report any change in foreign ownership, control, or influence (FOCI) is met through the submission of a *revised SF 328*. SF 328 is the enigmatic "CSA designated form" mentioned in 1-302h (5). The form is all that's required; however, a cover letter explaining the reason for submission of any form is always helpful.

Reports to the CSA under 1-303 also go *to the DSS Field Office*. Paragraph 1-303 has two basic purposes: 1) To establish an "in-house" reporting system to ensure that the FSO is aware of any loss, compromise, or suspected compromise of classified information and 2) to outline the reporting requirements should such an event occur. There should, of course, be a system already in place to notify the FSO of any changes affecting the FCL, or any changes affecting PCLs (and LAAs), or any changes or conditions that appear likely to affect the facility's ability to safeguard classified information. As you might expect, though, reports of individual culpability (blame or guilt) for a security violation, described in 1-304, go *to DISCO!*

So there you have it. Reports on people go to DISCO; reports on the facility go to the DSS Field Office. The only snag is when the *person* is also identified with the *facility* as a Key Management Person (KMP). As we pointed out in Lesson 3, a KMP has a direct bearing on the Facility Security

Clearance. So reports about changes in the information previously submitted for your facility's KMPs are sent *to the DSS Field Office* under NISPOM, 1-302h(3). In all other respects, reporting on KMPs is the same as for any cleared employee. If any of the employee reporting situations occurs such as suspicious contact, death, termination of employment, becoming an RFI, etc. then you are to report the matter *to DISCO (with a courtesy copy to your DSS Field Office)*. It's still a very simple formula to remember:

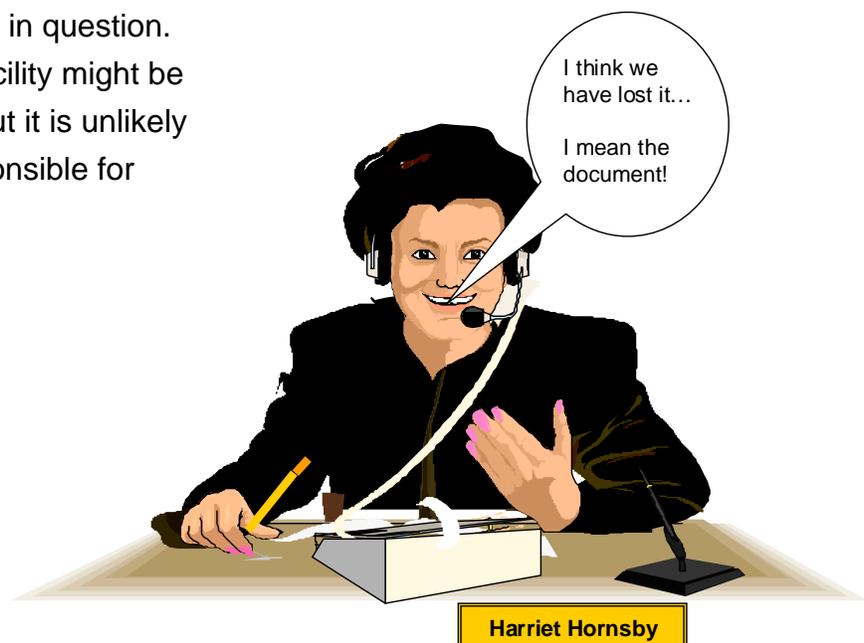
Reports on people, *including KMPs*, go to DISCO (copy to DSS Field Office).

Reports on the facility, *including KMPs*, go to the DSS Field Office.

REPORTS OF LOSS, COMPROMISE, OR SUSPECTED COMPROMISE

As this module is directed mainly at the non-possessing facility, we will not dwell in any great detail on reports of loss, compromise, or suspected compromise. Such reports would most commonly be generated by the facility possessing the classified information in question.

A non-possessing facility might be involved indirectly, but it is unlikely that it would be responsible for this report.



The basis for a report of loss, compromise, or suspected compromise (NISPOM, 1-303) is essentially the journalist's "big six; "**Who, What, When, Where, Why, and How.** Upon initial discovery that some piece of classified information or material has been lost, compromised, or suspected to have been compromised, the FSO must initiate a **preliminary inquiry** to ascertain all of the circumstances surrounding the reported loss, compromise, or suspected compromise and notify the DSS Field Office immediately. This notification may be accomplished by a telephone call or email to the Industrial Security Representative (ISR). The **initial report** to the DSS Field Office should give the facts as they are then known. The **final report** will be submitted upon completion of the *contractor's* inquiry—normally within 15 days after submission of the **initial report**. The DSS ISR will provide a suspense date to the FSO for submission of the **final report**. The required contents of the final report are shown in the chart on the next page.

If your DSS Field Office determines that more information is necessary to fully describe the situation, an IS Rep may be sent to the facility to conduct an Administrative Inquiry. If the completed report indicates loss, compromise, or suspected compromise of classified information, the User Agency (Government Contracting Agency) will be notified and asked to evaluate the classified information and to assess the damage done.

CONTENTS OF FINAL REPORT

Required Contents of Final Report to the CSA (DSS Field Office) for Incidents of Loss, Compromise, or Suspected Compromise:

Reference the initial report.

Describe material involved to include originating activity or contractor (name and address), date of origin, document title, number of pages, description of contents, contract or program under which material was received or produced and classification level of the information.

Give the essential facts of the incident: Where, when and how it occurred and any contributing factors.

Give the name, position, social security number, date and place of birth and date of PCL or LAA of individual(s) primarily responsible for the incident, along with a listing of any previous such incidents or any previous failure to comply with the NISPOM for which the individual was responsible.

Identify the person who first reported the incident and state when and to whom it was first reported.

State what action was taken to secure the material and to limit any damage after the violation was discovered. Include names and dates.

Describe when, for how long and under what circumstances classified information was vulnerable to unauthorized disclosure. List any unauthorized persons who may have had access to the information at that time.

Identify any classified documents or materials which are lost or unaccounted for.

Give specific reasons concluding that:

- 1) Loss or compromise occurred *or*
- 2) Compromise is suspected *or*
- 3) The probability of compromise is considered remote *or*
- 4) Compromise did not occur.

State what actions have been taken to prevent any recurrence of similar incidents.

State what disciplinary action, if any, was taken against the individual(s) responsible.

State whether or not the SPP (if applicable) was followed. Was the SPP adequate? If not, how was it inadequate and who was responsible for the inadequacy?

ADVERSE INFORMATION REPORTING

Of all the reports you, as FSO, are responsible for, the report of adverse information (NISPOM, 1-302a) may well be the most important.

WHAT IS AN ADVERSE INFORMATION REPORT?

Essentially, it is a report concerning a cleared person, reflecting upon that person's ability to safeguard classified information. Many aspects of an individual's character are considered before he or she is granted a clearance for access to classified information. Considerations include:

- the cleared employee's financial situation,
- reliability as evidenced on the job,
- reliance on drugs or alcohol,
- criminal convictions,
- indeed, *any* factor affecting a person's judgment, suitability, or reliability.

You will note that the examples given here are the same as those given in Lesson 4. This is because the PCL process, as we explained in that lesson, is an ongoing process not a final determination. The adverse information report is simply another way of ensuring that a cleared person may continue to be trusted with classified information.

WHO MAKES THE REPORT AND HOW IS IT MADE?

Ultimately, the FSO makes the report. But first, the information has to get to the FSO. A system must be put in place to forward information to the FSO. The basis of this system is the education of the employees. An employee who does not understand the nature or purpose of the report, who does not comprehend its importance to the national security, who fears exposure or reprisal for making the report and therefore fails to report, will jeopardize the effectiveness of adverse information reporting as a tool in protecting the national defense.

It is necessary, therefore, to reassure employees that an adverse information report will be treated as a confidential report, if so requested under the Privacy Act. The subject of the report need never know who the originator was.

Employees aware of adverse information often fear that their report will result in the firing of the subject, who may well be a friend as well as a co-worker. This almost never happens. An adverse information report is looked at as only a part of the overall picture. If the disclosed information warrants it, a report may generate the reinvestigation of a person's background, not unlike the periodic reinvestigations which are already part of many clearances. If the investigation turns up evidence of untrustworthiness, the PCL may be terminated. Whether this action has any bearing on that person's continued employment at the facility is a matter for that company's management to determine.

To re-emphasize: *A single adverse information report is unlikely to result in the revocation of a PCL or the subsequent loss of a person's job.* As for educating employees to the importance of adverse information reporting to the maintenance of security, this is part of your most important job, the education and training of the people in your company. If they understand the importance of maintaining national security, if they understand how they fit into the larger scheme of things, if they understand specifically how they, in the course of their duties, protect and safeguard classified information, then they can understand and respect the need for adverse information reporting and they will make those reports called for by paragraph 1-302a of the NISPOM.

In addition to education of employees, there are other methods to ensure adverse information is reported to the FSO. Many of these systems require absolutely no judgment calls on the part of any individual. For example, garnishment of wages, a situation generally known by the Personnel Officer, should be made the subject of an automatic report to the FSO. The same would apply to any knowledge of a criminal conviction. Other situations are trickier. Voluntary enrollment in an alcohol rehabilitation program is not cause for the generation of an automatic adverse information report. However, failing to maintain sobriety on the job, whether or not the individual is enrolled in a rehabilitation program, is.

DO ADVERSE INFORMATION REPORTS REALLY DO ANY GOOD?

Unquestionably, they do. They act as a barometer to help identify individuals whose continued access to classified information requires reassessment. Frequently adverse information reports *do* result in reinvestigations, and in some cases clearances *are* terminated.

CAN ADVERSE INFORMATION REPORTS PREVENT SPIES?

Going back to examples of espionage that we know have occurred in the past, we can see clear instances of where adverse information reporting *might* have prevented or decreased the resultant damage.

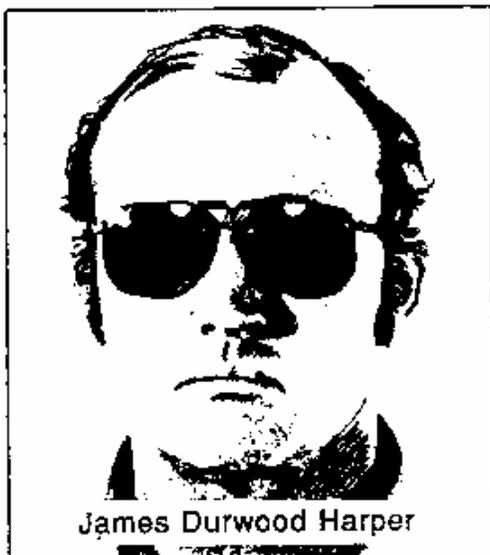
Take the case of William Holden Bell. It was known to at least a few of his fellow workers that he had financial difficulties (which suddenly disappeared) and that he was associating with a Polish national. Both were circumstances that could have been reported. Bell's case points out an important aspect of adverse information reports concerning finances: It isn't only the conspicuous display of newly acquired wealth, which is revealing. The sudden and unexplained removal of large debts and financial obligations also says a great deal about a

person's financial situation. Had either Mr. Bell's finances or his association with Marion Zacharski, (a polish national) been reported, a reinvestigation of Mr. Bell would almost certainly have ensued. It is impossible to state that the reinvestigation would have uncovered the espionage, but surely, at the very least, just knowing that he was being investigated would have dampened Mr. Bell's enthusiasm for spying.



William Holden Bell

An even more blatant example of a situation where adverse information reporting should have occurred was provided by Ruby Louise Schuler. She was the wife of James Durwood Harper. While he was the "mastermind" and handled all the James Bondian matters, *she* was the one with access to classified information. Mr. Harper did not have a Personnel Security Clearance or the means to directly access any of this nation's classified information. But through his wife, who held a clearance with a defense contractor, he was able to get his hands on 200 pounds of classified documents. It was his wife, Ruby, who should have been the subject of an adverse information report. As it happens, she wasn't, in spite of the fact that her alcoholism was well known to her co-workers. She was seen during the day drinking from a miniature bottle of vodka which she kept in her purse. An adverse information report filed on Ruby's alcohol problem could have led to the revocation of her clearance long before she met and married Harper. If nothing else, it would have put her on notice that her behavior and conduct were being observed, which would in turn have made Harper more cautious. And such concern might have helped Ruby. She died of cirrhosis of the liver.



James Durwood Harper



Ruby Louise Schuler

CHART OF REPORTS

On the following pages you will find a chart of the reports required by the NISPOM. The chart tells you the NISPOM reference, the title of the report, the circumstances under which it is sent, the format of the report, and where to send it.

BASELINE REPORTS



NISPOM	Report Title	When to Send	Form of Report	To
1-301	"Espionage," "Sabotage" or "Subversive Activity"	Upon learning of existing or threatened espionage, sabotage, or subversive activities at any of the contractor's sites	Letter. If the matter is urgent, make an initial report by phone. Follow up with written report. Send a copy to the DSS Field Office	FBI or DSS Field Office
1-302a	"Adverse Information"	<p>Upon learning information that adversely reflects on the integrity or character of a cleared employee, which suggests that his or her ability to safeguard classified information may be impaired or that his or her access to classified information clearly may not be in the interest of national security, such as</p> <ul style="list-style-type: none"> • Criminal activities • Treatment for mental or emotional disorders • Excessive use of intoxicants • Use of illegal, controlled substances, such as marijuana, heroin, cocaine, and hashish • Excessive indebtedness or recurring financial difficulties <p><i>Reports based on rumor or innuendo should not be made.</i></p>	<p>Letter, on company letterhead or with company's names and address, addressed to DISCO, ATTN: Chief Special Programs Branch, to include:</p> <ul style="list-style-type: none"> • Date of submission • Subject's last name, first name and middle name • Social security number • Date and place of birth • Clearance level and date of clearance • Home address • Facility code where the clearance is held • Reporting facility's code • Subject's physical worksite • Employment status (if terminated, add termination date) • Adverse information being reported (If garnishment, please list date of garnishment, court, amount and complainant, or attach a copy of the garnishment order) • Name and telephone of the person to contact for further information • Signature, typed name and title of the person submitting the report. 	<p>D</p> <p>I</p> <p>S</p> <p>C</p>
1-302b	"Suspicious Contacts"	<p>When any individual, regardless of nationality, tries to obtain illegal or unauthorized access to classified information or to compromise a cleared employee.</p> <p>_____ or _____</p> <p>When there is contact by a cleared employee with known or suspected intelligence officers from any country.</p> <p>_____ or _____</p> <p>When there is any contact which suggests the employee may be a target of an attempted exploitation by the intelligence officers of another country.</p>	Letter. If the matter is urgent, make an initial report by phone. Follow up with written report.	<p>O</p>



BASELINE REPORTS 3

NISPOM	Report Title	When to Send	Form of Report	To
1-302h	"Changed Condition Affecting the Facility Security Clearance"	1) Change of ownership 2) Change of name or address 3) Change to information previously submitted for KMPs 4) Termination of business 5) Change in FOCI: <ul style="list-style-type: none"> - Anticipated change - Actual change 	Letter Letter Letter to include: <ul style="list-style-type: none"> • Names of KMPs being replaced (if any) • New KMPs date and place of birth, social security number and citizenship • Whether new KMPs have been excluded from access, or temporarily excluded pending granting of their PCLs Letter. Letter. Letter. Include copy of Schedule 13 D if received. Revised SF328	D S S F I E L D O F F I C E
1-302m	"Employee Information in Compromise Case"	Upon written request of DSS Field Office	Letter. Contents determined by DSS Field Office	
1-303	"Loss," "Compromise," or "Suspected Compromise"	Upon loss, compromise, or suspected compromise of classified information	See discussion and report contents, pp.6-6-7.	
1-304	"Individual Culpability Report"	When individual responsibility for a security violation can be determined and one or more of the following factors are evident: <ul style="list-style-type: none"> • Deliberate disregard of security requirements • Gross negligence in the handling of classified material • A pattern of negligence or carelessness 	Letter that includes a statement of the administrative actions against the employee.	D I S C O

EXAMPLES OF VARIOUS TYPES OF REPORTS



To close, we're going to look at some examples of conditions and circumstances that require reports of one sort or another. It's up to our friend Harriet (the FSO) to decide if a report is, in fact, needed and how that report should be made.

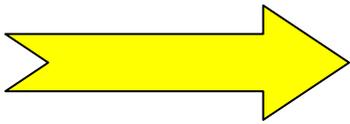
1) **Jimbo Duggins**, a widget repairman cleared **SECRET**, has been having financial troubles. As a result, his wages have been garnished. Harriet is aware of this because Wanda Fishtank, who handles personnel matters, has been instructed to keep Harriet apprised of problems of this sort.

JIMBO DUGGINS

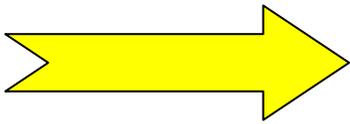
- 2) **Electric Widget Services** will be moving in four months from Wombat Heights to Drawstring Hollow. Harriet just received the mimeographed memo that was sent out to all employees. She's very busy right now and wonders if she can put matters off a bit.
- 3) **Roberta Baloon** has a **CONFIDENTIAL** clearance and has just had her name legally changed to Bobbie Baloon.



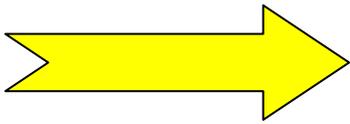
ROBERTA BALOON



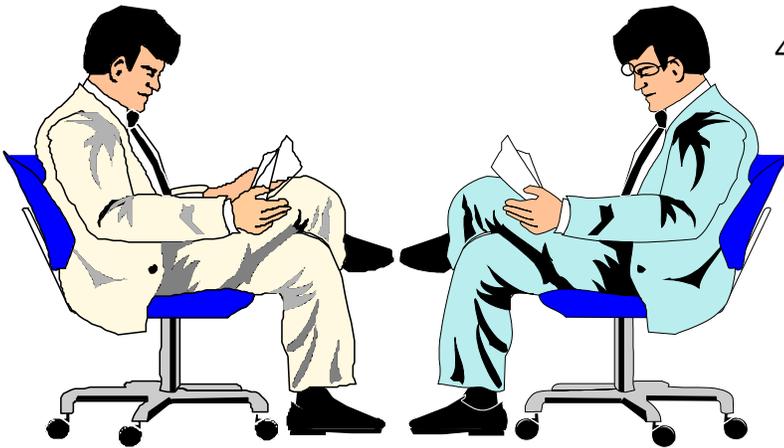
Harriet should file an adverse information report with DISCO, providing all of the information required by **1-302a** and paying particular care to see that the required details concerning the garnishment are all included. **(1-302a, NISPOM)**



She should let the DSS Field Office know right away, by letter, before it slips her mind. The records will be amended at the DSS Field Office to reflect the forthcoming change of address. An IS Rep will conduct a new survey/review when EWS moves in. **(1-302h(2), NISPOM)**



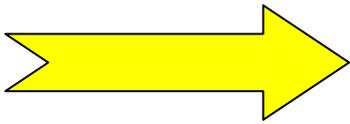
A simple DISCO Form 562 noting Roberta's name change will suffice. This should be transmitted to DISCO using EPSQ. **(1-302c, NISPOM)**



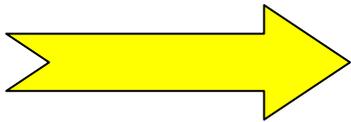
4) **Walter Wilbersnoot**, Harriet's boss, tells her that his twin brother **Waldo**, the world traveler, has started an oriental rug business in Bucharest, Romania. Waldo has asked Walter to represent the firm in marketing the products it is planning to export to the United States.

5) After thirty years with the company, **Willona Riggs** is retiring. She has held a **CONFIDENTIAL** clearance for three years.

6) **The Electric Widget Company** is considering distribution of some of their unclassified widgets to Eastern European countries. Does Harriet have to concern herself in this matter?



Since Mr. Wilbersnoot is cleared (at the SECRET level), Harriet needs to submit a 1-302d report, Representative of a Foreign Interest, to DISCO. The report should describe the nature and extent of his activities on behalf of his brother's foreign firm. (1-302d, NISPOM)



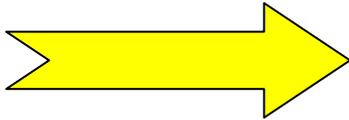
Harriet must debrief Willona (3-108, NISPOM). Then Harriet needs to complete a DISCO Form 562 (Termination of employment) and transmit it to DSS using EPSQ. (1-302c, NISPOM)



No. EWS is a branch office of the Electric Widget Company. The report, in the form of an advisory letter to the DSS Field Office, will be submitted by Harold Huxtable, EWC's FSO. (1-302h(5), NISPOM) Matters will be handled by the DSS Field Office in Harold's region. If the distribution plan goes through, then Harry would submit a new SF 328 to the DSS Field Office. Should the change in FOCI be enough to adversely affect the control of EWC (an unlikely event in this case), the DSS Field Office would work with EWC to attempt to negate the FOCI, if at all possible. (2-305, NISPOM)

7) Mr. Wilbersnoot thinks Harriet is overworked. Being FSO is only one of her many jobs. He tells her that he's appointing Wanda in her place.





Harriet needs to report a change in KMPs to her DSS Field Office. Since EWS is a branch office, the only personnel considered KMPs are the branch manager and the FSO. As Wanda is going to be the Facility Security Officer, she should be included in the report. (Wanda held the post for two weeks, until she realized just how much work was involved in being an FSO. She subsequently resigned. Harriet is once again the FSO.) (1-302h(3), NISPOM)



SUMMARY

The FSO informs appropriate government elements (the FBI, the DSS Field Office, DISCO) of significant events and circumstances at the facility by submitting various reports and documents. There are three basic categories of reports; 1) those concerning changes that affect the FCL or PCLs; 2) those conveying adverse information; and 3) those reporting the loss, compromise, or suspected compromise of classified information. As a general rule, reports on people, including KMPs, go to DISCO, while reports on the facility, including any change to the information previously submitted for KMPs, go to the DSS Field Office. The most common reports to DISCO are made on DISCO Form 562, while most reports to the DSS Field Office are made by letter. Adverse information reports provide an important means of identifying individuals whose continued access to classified information may require reassessment.

For the following questions, refer to the charts on pages 6-13, 14, and 15.

4. Ozbak Pleebo, an immigrant alien with a CONFIDENTIAL LAA, is anxiously waiting to become a US citizen. When this happens, who must be notified? _____
By what means? _____

5. Tragedy struck the annual Digital Widgets-Gizmo Corp. softball game. While rounding third, old Mr. Appleby, the Treasurer at Digital, dropped dead. "It's how he would have wanted to go," said Mrs. Appleby. What sort of report(s) must be made and where should the report(s) be sent?

6. Mr. Wilbersnoot told Harriet, our FSO, that he was off to a meeting of the Association of Widget Engineers (AWE). The topic this year is "A Fuller Life Through Widgets." The meeting will be in Melbourne, Florida. Only members of the Association will be in attendance and all Association members are American citizens. Does Harriet have anything to report?

7. Hank Windles, an engineer holding a SECRET clearance at Digital Widgets, was found face down on his desk. At first, his fellow workers attributed this to boredom. Then they saw the bottle of peach brandy. This was not the first time that Hank had been discovered in this condition at work. In fact, these incidents were becoming quite frequent. What actions should be taken?

8. George Porgee, IS Rep, drove out to Widget Wiring Supplies in Wahoo, Wyoming for that facility's government review. He turned his car into the lot and saw, to his dismay, absolutely nothing! Widget Wiring had moved the month before. What should the company have done before the time of the move?

9. "It was right here a minute ago!" wailed Leonard. But no one could find the classified widget. Who must be notified of the loss?

10. Mild-mannered Miss Violetta Lambkins had worked as a cleared secretary at Gizmo for 35 years. It was therefore quite upsetting when Mr. Henway walked in on Violetta as she was taking photographs of a classified document with a tiny camera. Who should be told of this shocking incident?

11. When Harriet answered the telephone at three o'clock in the morning, she was surprised to hear Mr. Wilbersnoot on the other end. He sounded awfully shaken. He and some of his fellow AWE members had chartered a plane down in Florida to do a little post-conference sight-seeing. And one of the group, after too many margaritas, had hijacked the craft to Cuba. Luckily, they were all quickly returned to the US. Not, however, before the Cubans questioned Mr. Wilbersnoot rather thoroughly about his line of work. What does Harriet do now?

6 - Solutions & References



1. changes, adverse information, loss, compromise, suspected compromise.
(pp. 6-2,)
2. d. (p. 6-9,10)
3. True. (p. 6-5)

The NISPOM references given below are on pp. 6-14,15,16.

4. DISCO. DISCO Form 562. (1-302e, NISPOM)
5. A DISCO Form 562 (death of employee) should be sent to DISCO (1-302c, NISPOM)
6. No.
7. The employees should notify the FSO and the FSO, in turn, should send an adverse information report to DISCO. (1-302a, NISPOM)
8. A changed condition report (change of operating address) should have been sent to the DSS Field Office. (1-302h(2), NISPOM)
9. The FSO, who should then notify the DSS Field Office. Immediately. (1-303, NISPOM)
10. The FBI should be notified immediately, by telephone and followed up in writing with a copy to the DSS Field Office, (1-301, NISPOM).
11. She should send a report of the matter to DISCO. (1-302b, NISPOM)

LESSON 7

Procedures for Visitors

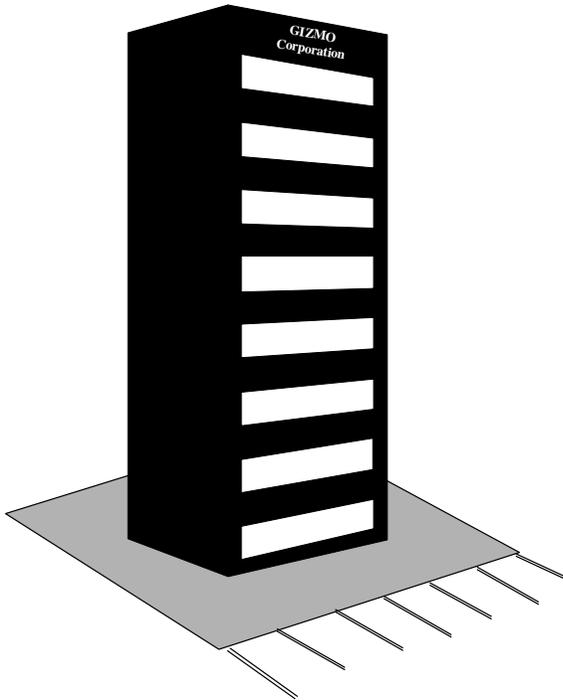
A "classified visit," as defined by the NISPOM, refers to a visit where the visitor requires access to classified information. As we are dealing in this course with non-possessing facilities, we are going to look only at those visit control procedures that apply to a visitor from a non-possessing facility who is visiting a possessing facility or government activity, where he or she will have access to classified information. This lesson will **not** address the control of visitors at a possessing facility, which is the other side of the coin.

OBJECTIVES

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

- Define a visit under the terms of the NISP.
- Complete a visit authorization letter for a visitor from one facility to another facility.
- Given a situation, decide whether contract related or non-contract related visit procedures apply.
- Follow through on the steps involved in either the contract related or non-contract related visit.

CLASSIFIED VISITS



We are concerned only with a very specific sort of visit. A visit, as we are defining it here, is a visit that involves access to classified information. Since this volume is directed primarily at facilities which do not keep classified materials or information in-house, our concern will be with those cleared personnel who will be visiting another cleared contractor's facility or a government agency to gain access to classified information.

We have said that the purpose of a classified visit is to access classified information. Note, however, that in some instances the visit itself may not require access to classified information, but the visitor cannot be successfully isolated from classified material that the host may have on site. For example, a serviceman might have to board a ship in order to repair a piece of equipment that cannot be removed. If, in order to repair the equipment, he has to work in a compartment or cabin that contains information classified SECRET and adequate measures cannot be taken to prevent him from gaining knowledge of the classified information, then the serviceman must have a clearance at the SECRET level, even though he has no direct concern with the other mysterious equipment, personnel, or activities in the area in which he is working. If the visitor cannot be excluded from access, then the visit becomes a classified visit and all the requirements that are associated with such a visit must be met.

CONTRACT RELATED VISITS

Under the NISPOM there are two distinct types of visits.

A *contract related visit* is a classified visit by an employee of a cleared contractor to another cleared contractor or User Agency with which the employee's company has a *classified contractual relationship*. Remember that the definition of a classified contract includes all phases of pre-contract activity (see **Appendix C, NISPOM**). Therefore, a visit to a prospective subcontractor may be considered a contract related visit. However, a formal or written solicitation (Request for Proposal, Request for Quote, or Invitation for Bids) must have been issued, or the contractor must otherwise have been furnished authority by the UA to disclose its classified information.

With classified visits, as with Personnel Security Clearances, it is necessary to keep the number down to the very minimum needed to do a job. This is not only better from the government's standpoint, but it also makes your job easier if there are fewer classified visitors to keep track of. Your counterpart at the host facility similarly benefits, as he or she is not responsible for an excessive number of visitors having access to classified information at his or her site.

To return to Electric Widget Services (EWS): Suppose Harriet, our FSO, is contacted by someone in the Service Department who says that the Gizmo Corporation has called to report a broken widget. The widget, which is repaired on site, has a SECRET level

classification. What steps does Harriet take to send a serviceman to Gizmo?

First, she must establish that access to classified information will be required to achieve the purpose of the visit. This may be determined in one of two ways. 1) Usually the need for access is determined from the Contract Security Classification Specification (DD Form 254) itself. 2) It may also be determined based on a notification from the host activity. Next, she must confirm that the serviceman to be sent is cleared to the SECRET level. Then she must complete a *visit authorization letter* (normally a letter) for the person in question. We'll go over the contents of the visit authorization letter shortly. The visit authorization letter is sent to the Facility Security Officer of Gizmo Corp., Wellington Minor. Wellington then has the responsibility of confirming the clearance of EWS. If this is the first time that EWS is being employed by Gizmo in its capacity as a cleared facility or if Wellington believes there may have been a change in EWS's FCL status, he confirms EWS's clearance by placing a telephone call to the Defense Security Service - Central Verification Activity (DSS-CVA). Or registering to go on-line and verify FCLs at www.dss.mil. Once the FCL status of the visitor facility has been established, *it is not necessary to repeat this procedure for every visit*. However, if there is ever any question as to the validity of a visit authorization letter, the DSS Field Office of the visitor's facility should always be contacted. Call the Security Department of the facility to get the telephone number of the local DSS Field Office.



JIMBO DUGGINS

If Gizmo Corp. calls the DSS-CVA, personnel there will check its computerized facility files to confirm the clearance level of EWS. Based on this confirmation or on an existing classified contract between the firms and on EWS's assurance, through the visit letter, that the serviceman is cleared, Gizmo Corp. may now OK the visit authorization letter. It is always up to the host facility to accept or deny a visit authorization letter. Normally, Gizmo Corp. would not call Harriet unless the visit authorization letter was *disapproved*.

After Harriet forwards the visit authorization letter to Gizmo, she tells the serviceman, in this case Jimbo Duggins, to go out to Gizmo on the date specified in the letter. She reminds him to carry some valid form of identification with his name and photo, such as a driver's license. Harriet retains a copy of the original visit authorization letter sent to Gizmo, and she keeps it on file until the visit has been completed. In this way she has a record of which cleared personnel are out on classified visits and where the visits are being made.

DSS/Central Verification Activity

**Go to www.dss.mil and click on "LOC, CVA & DCII."
Then follow the instructions on the screen.
You may also call the CVA at 1-888-282-7682**

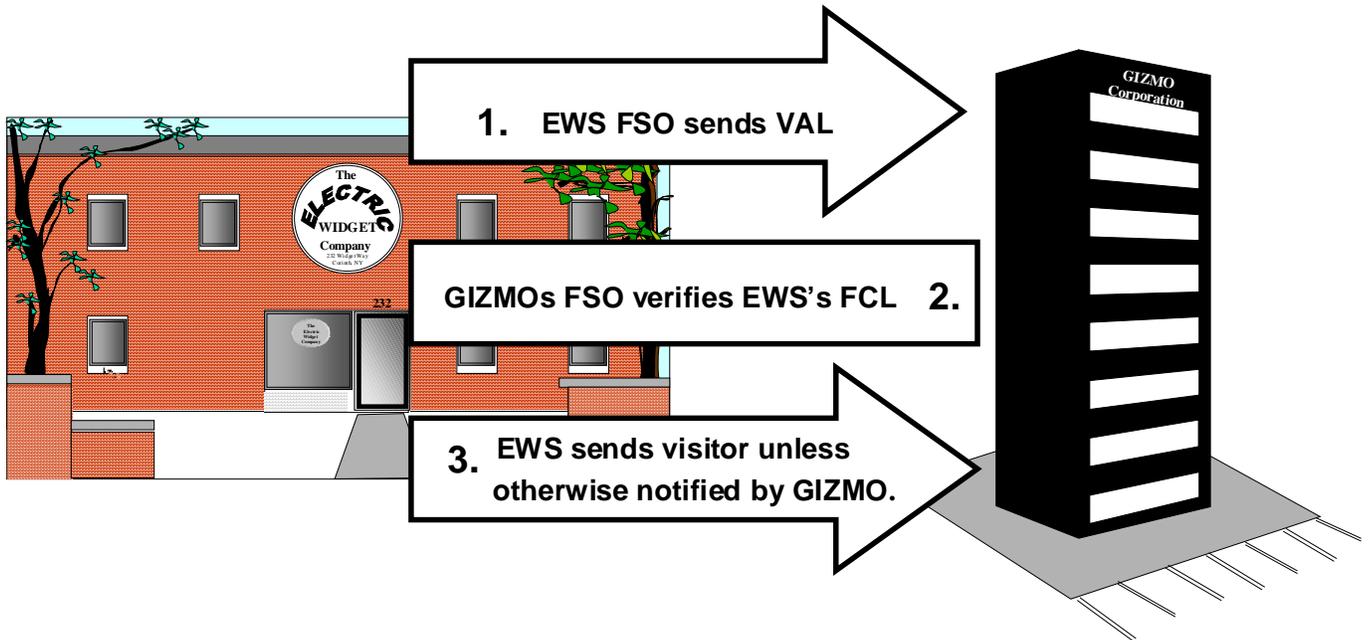
NON-CONTRACT RELATED VISITS

The difference between contract related visits and non-contract related visits is in the relationship between the contractor sending the visit authorization letter and the host contractor or host User Agency. If there is *no classified contractual relationship* between the sending contractor and the host, the visit is *non-contract related*.

Non-contract related visit procedures are the same as for contract related visits, except that the *facility making the disclosure is required to obtain disclosure approval from the User Agency that owns the specific information*. This certification is retained by the facility making the disclosure. *Note: This could be either the visitor's facility or the host facility.*

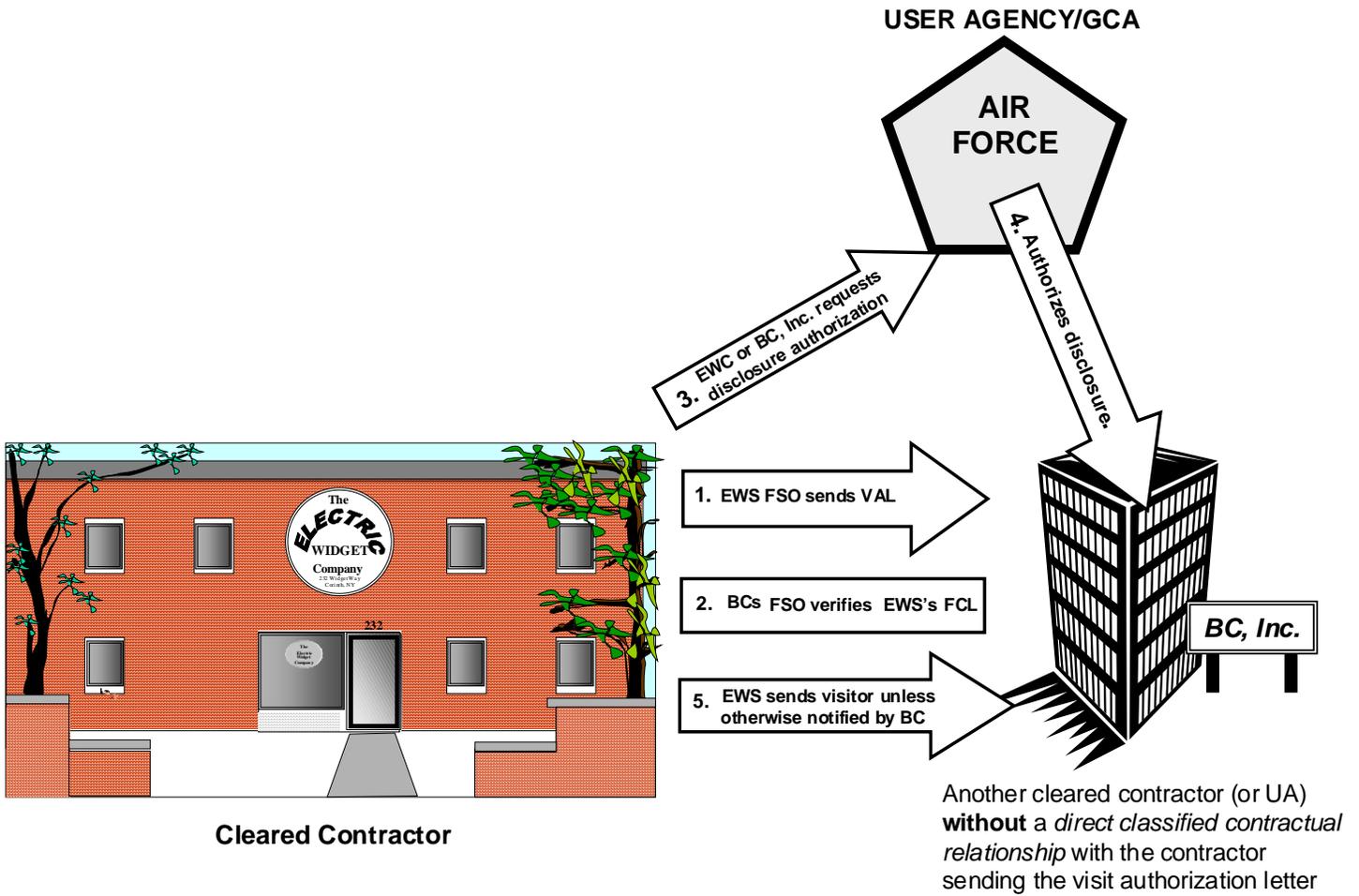
An example of a non-contract related visit would be when someone from EWS goes to visit Bowling Center, Inc. (BC). EWS and BC have no classified contractual relationship. BC is involved in the Air Force's Snark Project and has been furnished modified EWC widgets by the Air Force. The Air Force will probably contract with EWS to service the widgets once they begin taking delivery of Snark systems. EWS must meet with BC to determine how EWS personnel can service the EWC widgets which, in the Snark Project, will be encased in BC classified components.

CONTRACT RELATED VISIT



Another cleared contractor (or UA) **with** a direct classified contractual relationship with the contractor sending the visit authorization letter

NON-CONTRACT RELATED VISIT



THE VISIT AUTHORIZATION LETTER

In addition to simply serving notice that a visit is forthcoming, a *visit authorization letter (VAL)* serves the following purposes:

- First, it allows the company being visited to confirm the clearance status of the company sending the VAL. We saw how this worked in the section above.
- Second, it gives the clearance level of the visitor, as vouched for by the FSO of the visitor's company. This information is incorporated into the request itself, along with a great deal of other information.
- Third, it provides the visitor's company a means of keeping track of their personnel who are out on classified visits. This can be easily done by filing a copy of the VAL. In this way, the FSO can identify any of the company's classified visitors should the need arise.



EXTENDED VISIT AUTHORIZATION LETTER

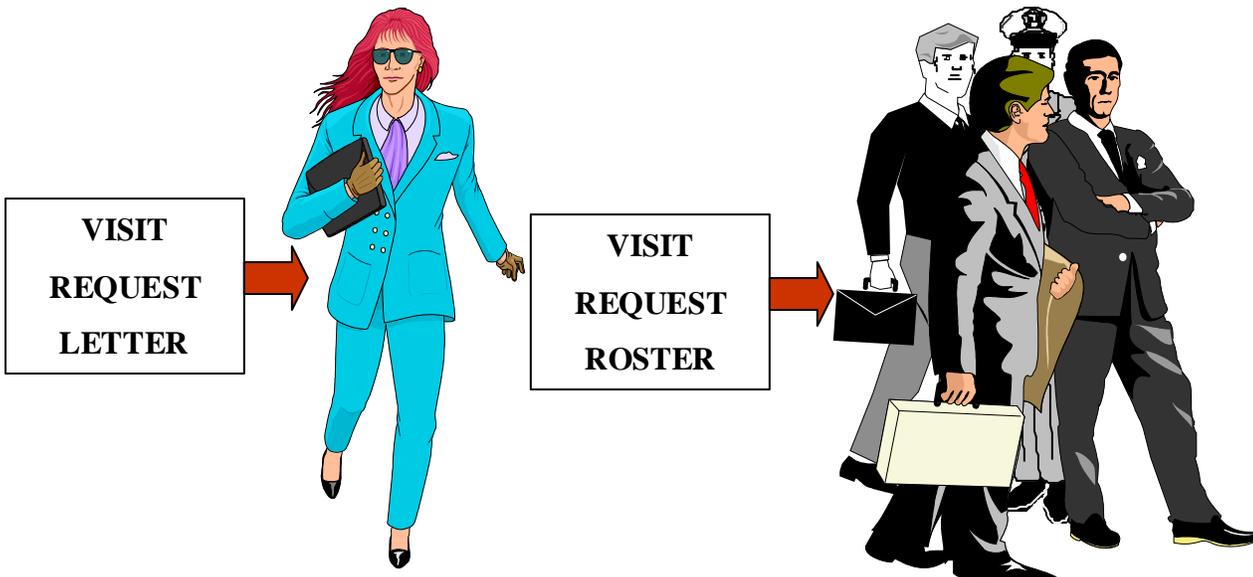
If several visits to the same place will be needed for up to a 12-month period, a single visit authorization letter may be submitted to cover all of the visits for the period. For contract related visits, the VAL may be approved for the life of the contract (see **NISPOM, 6-104**). The FSO of the visitor's facility is obligated to contact *all host facilities* with which such an extended VAL is in effect in the event of two types of changes: 1) changes in the *status of the visitor*, such as termination of employment, suspension, leave of absence, and the revocation or termination of the employee's clearance; and 2) changes in the *status of the visitor's company*, such as a change in the level of FCL or change of the FCL to a limited clearance.

So keep in mind when making a report, if the report is on an employee who makes classified visits under an extended visit authorization letter, *all* such host facilities should be notified. And if there is a change in your facility's security clearance, *all* host facilities with which you have an extended VAL arrangement should be notified.

FORMAT

A visit authorization letter must contain the six basic elements listed in paragraph **6-103** of the NISPOM and found on the following page. There is no set format for a visit authorization letter. The NISPOM elements may be made into a form for use by your company, especially if a great number of classified visits are usual for your firm. Or it may take the form of a standard business letter. The format is unimportant,

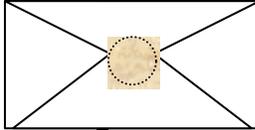
as long as all of the required information is provided. A sample of one VAL format is shown on page 7-13. If a large number of visitors are sent to a particular company, rosters may be incorporated into the format of the visit authorization letter. All of the required information must be provided for each person on the roster.



A visit request may be for one person

OR

For a number of people , if all required information is given for each person.



CONTENTS OF A VAL

There is no standard format for a visit authorization letter (VAL). Across the page is a sample of one format. All visit authorization letters must contain these six items.

- 1.** Requesting contractor's name, address, and telephone number, assigned CAGE Code, if applicable, and certification of the level of the facility security clearance. (If a limited clearance, so state.)
- 2.** Name, date and place of birth, and citizenship of the employee intending to visit.
- 3.** Requestor's certification of the level of personnel clearance of the proposed visitor and any special access authorizations required for the visit, such as NATO, CNWDI, or COMSEC. (If the clearance is interim or company-granted CONFIDENTIAL, or is an LAA, so state.) (Note that NISPOM paragraph 2-205 as ammended states, "As of January 1, 2004 contractor granted Confidential clearances will no longer be valid for access to any classified information.)
- 4.** Name of person(s) to be visited.
- 5.** Purpose and sufficient justification for the visit to allow for a determination of the necessity of the visit. (Including a specific contract number, project, or program number will assist the recipient in making this determination. Do not use nicknames, abbreviations, short terms, or acronyms.)
- 6.** Date or period during which the VAL is to be valid.

**Electric Widget Company
232 Widget Way
Corinth, New York 14623 1
716-555-0001**

May 23, 1999

Subject: VISIT AUTHORIZATION LETTER

Mr. Marvin Orthnic
Facility Security Officer
Gimcrack Enterprises, Inc.
707 Industrial Road
Baltimore, MD 21212

Dear Mr. Orthnic:

The following three EWC engineers will be at your facility the week of June 20 **6**
to meet with Donna Lloyd-Beckman, chief of your engineering department, **4**
to discuss the upcoming Zinnia Project (#N0042-43-0000). **5**

Visitors:

2
Selina K. Weller
Senior Engineer
14-11-57
Wendover, Nevada
U.S. citizen

Evan M. Pockley
Engineer
01-10-38
Canandaigua, New York
U.S. citizen

Walter C. Quom
Engineer
28-09-51
Raine, Louisiana
U.S. citizen

I hereby certify that the above individuals hold TOP SECRET clearances. **3**
EWC has a TOP SECRET Facility Security Clearance and our CAGE Code
is 9Q111. **1**

If any further information is required, please contact me at (716) 555-0021. **1**

Yours sincerely,

Harold P. Huxtable

Harold P. Huxtable
Facility Security Officer

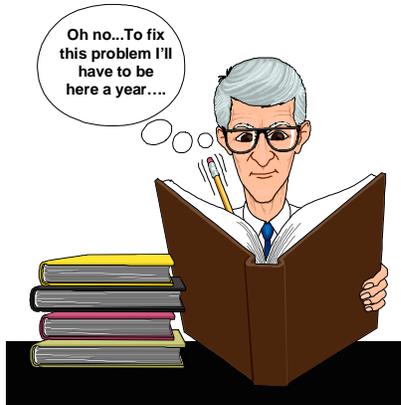


Visitor

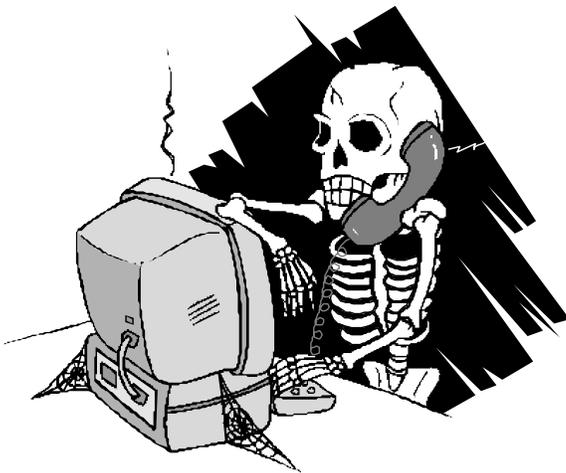
A visit authorization letter may cover a visit lasting for a day or less, a visit lasting for several days or more, repeated visits within a certain time frame—or visits throughout the life of the contract! An example of a brief visit would be one in which our repairman, Jimbo, pops over to Gizmo Corp. to replace a widget. The whole process takes only 1½ hours. If EWS had, say, a classified service contract with Gizmo that involved periodic maintenance, then EWS might issue a visit authorization letter to cover a certain period of time during which Jimbo could make repeated visits to Gizmo. Since Jimbo's visits to GIZMO are contract related, the VAL could be valid for more than one year.

Remember, VALs must always be submitted in writing. VALs may be sent by mail, facsimile, or teletype. Note: ***Note: Under no circumstances shall employee(s) be permitted to “hand-carry” their personal VAL(s) to the host facility.*** Such a procedure would not allow sufficient time for the host to verify required information for the visit. Additionally, electronic transmission including e-mail may be used. When using electronic means, access to the program must be controlled through physical or software protection and have digital signature authentication. If this capability is not available, the VAL must be sent via STU-III (a secure telecommunications unit). ***A telephonic request may be made in cases of genuine emergency, but it must be followed immediately by a written request.***

LONG TERM VISITORS



Long Term Visitor



Very Long Term Visitor

There is a special category of visit known as a long-term visit. This may involve more than merely the fact that the visit is of longer duration than usual. A long-term visit is one in which the employee of one company is physically located at another company for an extended period. An example of this type of visitor could be an electronics testing service, which sends employees to a cleared site to monitor equipment for the duration of that equipment's use. Or a temporary help supplier that sends specific administrative personnel to the same cleared site for an indefinite period. At EWS, an example might be when the company installs and monitors a SECRET widget at Gizmo Corp., the complexities of which require that a cleared EWS employee set up an office on-site for a year or more.

In all types of visits, the host is responsible for the visitor's actions regarding security. However long or short the stay of the visitors, each visitor must comply with the host facility's security procedures.

Golden Rule of Classified Visits

The security procedures of the host facility always rule.

WHAT YOUR EMPLOYEE CAN EXPECT DURING A VISIT

The DSS Field Office for the host facility always has the responsibility for the reviews. This office ensures that a visiting employee is properly safeguarding classified information and for notifying the host facility of any security violations on the part of that employee. In other words, when the time comes for the host facility's regular periodic review, the I.S. Rep(s) will check into the handling of classified visitors at that facility and check into how visitors (your personnel) are handling classified information at that facility. Just as it is the DSS Field Office's responsibility to ensure that the host facility is in compliance with all security regulations, including those pertaining to classified visits. It is the host facility's responsibility to oversee those visitors at its site.

Some, if not most, of the procedures your employees will have to observe while visiting a cleared facility will be new to them. The procedures for a facility handling classified information are necessarily more complex than those for a non-possessing facility. In addition to the wide range of rules governing the actual handling of classified information, there may be other security procedures in place.



One procedure that your visiting employee will certainly encounter is the visitor record. This will probably be a sign-in sheet (visitor log) requesting, at minimum:

- Visitor's name,
- Name of the activity represented.
- Date of the visit.

The host company may also have a badge system.

The important thing to remember is that the host facility bears the responsibility, not only enforcing the appropriate regulations, but explaining the procedures, to the extent necessary, to your employee(s). The host may also provide any special briefings that may be needed. Contractors are required to maintain a record of all visitors to their facility who have been approved for access to classified information.

SUMMARY

Within the NISP, a classified visit entails the visitor having access to classified information at the place visited. A contract related visit is one in which a cleared employee goes to the location of another cleared contractor or User Agency with which the visitor's firm has a classified contractual relationship. On visits between contractors, the FSOs of both the sending and receiving facilities have procedural obligations in arranging for the visit. **The FSO of the sending facility is responsible for providing a visit authorization letter (VAL) to the receiving facility.** The FSO of the receiving facility makes the decision to accept or deny the proposed visit and, if the visit is accepted, the FSO must ensure that the visitor follows the receiving facility's SPP, if one has been established. A non-contract related visit is one in which there is no classified contractual relationship between the two cleared contractors or user agency. **A non-contract related visit requires that the facility making the disclosure obtain disclosure approval from the user agency for the specific contract the classified information is related to.** When an extended visit authorization letter is in effect, the FSO of the visitor's facility must contact the host facility whenever the status of the visitor or of the visitor's facility changes. When there is a classified contractual relationship between the host and the visitor, a VAL may remain in effect for the duration of the classified contract.

7 Review Exercises



Complete the following exercises for review and practice.

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

1. Within the NISP, a "classified visit" involves the visitor having access to classified information at the place visited.
 True. False.

2. A contract related visit is one in which there is a c_____ relationship between the two cleared contractors involved, or the cleared contractor and the User Agency involved.

3. The definition of "classified contract" includes pre-contract negotiations.
 True. False.

4. A classified visit in excess of thirty days always requires a long-term visit agreement.
 True. False.

5. A visitor must comply with the security procedures of the host facility.
 True. False.

6. For each type of visit, number the steps in their correct order. For steps that are the responsibility of the *visitor's facility*, circle VF. For steps that are the responsibility of the *host facility*, circle HF.

Contract related:

- _____ VF HF Approve visit (implied by no action to deny visitor) or deny visit (by written notification).
- _____ VF HF Confirm clearance status of visitor's facility.
- _____ VF HF Confirm clearance status of visitor.
- _____ VF HF Determine need for classified visit.
- _____ VF HF Control visitor's access during visit.
- _____ VF HF Send visit authorization letter.

Non-contract related:

NOTE: For this part, we have indicated that it is the host facility that will be disclosing the classified information.

- _____ VF HF Obtain disclosure authorization from the User Agency contracting officer for the specific contract the classified information is related to.
- _____ VF HF Approve visit (implied by no action to deny visitor) or deny visit (by written notification).
- _____ VF HF Confirm clearance status of visitor's facility.
- _____ VF HF Confirm clearance status of visitor.
- _____ VF HF Determine need for classified visit.
- _____ VF HF Control visitor's access during visit.
- _____ VF HF Send visit authorization letter with UA/prime contractor certification.

7. Colonial Widgets is under contract to Worldwide Widgets to distribute classified widgets in parts of Virginia and Maryland. George Washington Beniker, president of Colonial, will be going out to Worldwide soon to look at the new line of classified widgets.

This describes a _____ visit.

8. What does Colonial's FSO do in connection with George's proposed visit?

9. George got a call recently from Major Wingwright of the Air Force, advising him that there was a problem with the new classified widgets they received. It seems that the widgets were too small for the classified widget handles manufactured by Widget Accessories, Inc. George opined that the widgets were the right size. It was the widget handles that were too large. Maj. Wingwright suggested that George get together with someone from Widget Accessories and hash everything out. Maj. Wingwright indicated that an exchange of classified information would be involved. George knew that Widget Accessories was unaware of Colonial's involvement in the Air Force program.

If George visited Widget Accessories, it would be a _____
_____ visit.

10. What steps must Colonial's FSO take?

11. Polly Graham is on a classified visit to Bemis Co. under an extended visit authorization letter. While she is there, her FSO receives word that Polly has won the state lottery and is quitting her job, effective immediately. In addition to filing a report with DISCO, what must the FSO do?

7 - Solutions & References



1. True. (p. 7-2).
2. classified contractual. (p. 7-3).
3. True. (p. 7-3)
4. False. (p. 7-10; 7-14).
5. True. (pp. 7-15).
6. **Contract related:**

<u> 5 </u>	VF	<input checked="" type="radio"/> HF	Approve visit (implied by no action to deny visitor) or deny visit (by written notification).
<u> 4 </u>	VF	<input checked="" type="radio"/> HF	Confirm clearance status of visitor's facility.
<u> 2 </u>	<input checked="" type="radio"/> VF	HF	Confirm clearance status of visitor.
<u> 1 </u>	VF	<input checked="" type="radio"/> HF	Determine need for classified visit.
<u> 6 </u>	VF	<input checked="" type="radio"/> HF	Control visitor's access during visit.
<u> 3 </u>	<input checked="" type="radio"/> VF	HF	Send visit authorization letter.

Non-contract related:

- 4 VF (HF) Obtain disclosure authorization from the User Agency contracting officer for the specific contract the classified information is related to.
- 6 VF (HF) Approve visit (implied by no action to deny visitor) or deny visit (by written notification).
- 5 VF (HF) Confirm clearance status of visitor's facility.
- 2 (VF) HF Confirm clearance status of visitor.
- 1 (VF) HF Determine need for classified visit.
- 7 VF (HF) Control visitor's access during visit.
- 3 (VF) HF Send visit authorization letter.

NOTE: If the visitor's facility were the disclosing party, then the sequence would be 3, 6, 5, 2, 1, 7, 4.

(pp. 7-3--5).

7. contract related. (p. 7-3).
8. FSO confirms need for visit, verifies George's clearance level, and sends visit authorization letter to Worldwide Widgets. (pp. 7-3—4).
9. non-contract related. (p. 7-5).
10. The FSO must confirm need for visit, verify George's clearance level, request disclosure authorization for the classified information involved from the appropriate contracting officer at the Air Force GCA, and send a VAL to the host facility (Widget Accessories, Inc.). (p. 7-7).
11. Polly's FSO must notify the FSO at Bemis Co. of the termination of Polly's employment. (pp. 7-8—9).
12. The following item was omitted: Certification of the facility clearance level of EWS. (p. 7-10).

LESSON 8

Security Education: Briefings

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

OBJECTIVES

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

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

INITIAL COMPANY BRIEFING

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

INITIAL SECURITY BRIEFING

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

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

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

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

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

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

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

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

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

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

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

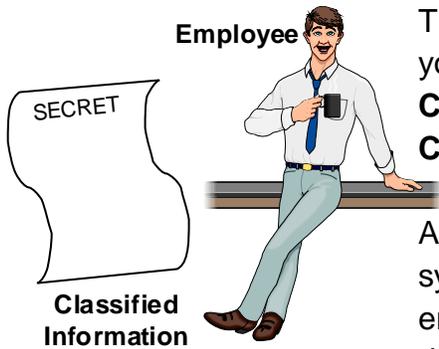
- **Damage** — CONFIDENTIAL
- **Serious Damage** — SECRET
- **Exceptionally Grave Damage** — TOP SECRET

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

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

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

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



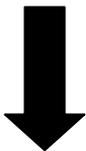
This is a tall order. If your facility possesses classified information, you will need to go over at least the requirements in **Chapter 4, Classification and Marking**, and **Chapter 5, Safeguarding Classified Information**, of the NISPOM.

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

Level of Clearance



Need-to-Know



Authorized Person

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

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

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

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

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

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

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

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

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

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

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

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

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



When in doubt find out...

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

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

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

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

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

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

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

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

EXECUTION OF SF 312

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

classified information and of the penalties for violating these obligations.

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

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

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

REFRESHER TRAINING



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

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

Helpful Hint: Vary your briefings to avoid boredom.

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

SECURITY DEBRIEFING

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

You must debrief cleared employees when:

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

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

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

SPECIAL BRIEFINGS

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

SPECIAL BRIEFINGS

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

SPECIAL BRIEFINGS - 2

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

SUMMARY

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

8 - Review Exercises

Complete the following exercises for review and practice.

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



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

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

_____ Usually given to both cleared and uncleared employees.

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

_____ Not required by NISPOM.

_____ Followed by execution of SF 312.

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

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

() b. making original classification decisions.

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

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

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

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

() True. () False.

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

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

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

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

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

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

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

8 - Solutions & References



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

LESSON 9

Initial Surveys & Security Reviews

In this lesson we'll first discuss surveys, which are done when a facility is initially cleared and when there is any changed condition that would affect the Facility Security Clearance (FCL). These are not inspections, but often a changed condition survey and a security review will be conducted simultaneously. You and the IS Representative will be working together during the survey review process.

Section II of the Security Agreement (DD Form 441) provides for designated representatives of the government to review the security program at your facility at reasonable intervals. The NISPOM paragraph 1-207 provides additional guidance regarding these reviews and also introduces the requirement for your company to conduct formal self-inspections at intervals consistent with risk management principals.

You probably want to know how to prepare for a security review, what will the results be, etc. We'll try to answer these questions, relieve any fears you may have, and help you maintain a good security program.

Besides discussing government reviews, their elements and results, we will discuss contractor self-inspections. We will discuss the NISPOM requirements as well as reasons for conducting self inspections, and how you can use the process to improve your company's security program.

OBJECTIVES

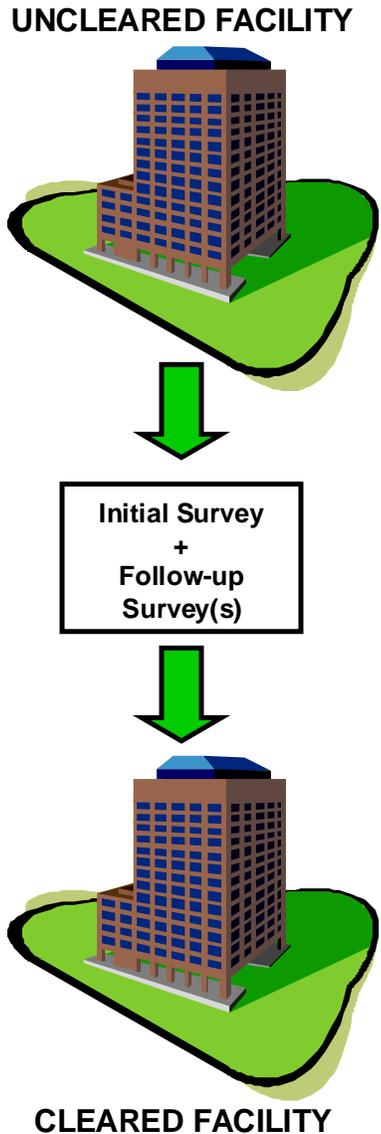
When you have finished this lesson, you should be able to do the following:

- List examples of instances where a "changed condition" survey is called for.
- List examples of when DSS will need to conduct a security review of a facility.
- Identify the areas of concern most commonly covered in the review of a non-possessing facility.
- Differentiate the ratings assigned upon completion of a review and indicate what results will be communicated to top management.
- Indicate when self-inspections are required.
- Explain how self-inspections are conducted.

THE INITIAL SURVEY

A survey is a tool used in the initial clearance of a facility and in the maintenance of that clearance. The *Initial Facility Clearance Survey* was conducted before your facility clearance was issued. The primary purpose of the initial survey was to gather information to determine that your facility was eligible for a clearance. The clearance of your firm was based on the five areas we went over in Lesson 3. The survey, however, focused on four of those areas:

- The Security Agreement
- Foreign Ownership, Control or Influence (FOCI)
- Your business structure
- Personnel Security Clearances (PCL) of Key Management Personnel (KMPs)



The initial survey began when DISCO sent out the basic facility clearance forms the DD Form 441 (the DD Form 441-1, if needed) and the SF 328. EPSQ software was also provided for your facility's KMPs to apply for PCLs. If your facility was near an IS Rep's office, he or she may have brought the forms by in person. However you received the forms, an IS Rep did come to your facility to pick up the completed forms, review the documents pertaining to your facility's business structure, and brief senior management on the National Industrial Security Program (NISP). Depending on the complexity of your facility's operations, a second visit, or *Follow-up Survey*, may have been scheduled. If needed, a third or even fourth visit might have been made. The important thing during the visit was to get your company's security program started.

When the clearances for your KMPs are ready to be granted, DISCO coordinates with the DSS Field Office and issues the Facility Security Clearance. Then DISCO electronically sends the Letters of Consent (LOC) for the KMPs coupled with the Letter of Notification of Facility Clearance (DSS FL-381-R), to your facility. At this point your facility is called, **a cleared facility**.

CHANGED CONDITION SURVEYS

Once the initial survey has been completed why should you be concerned with all of that now? Very simply, just as a personnel security clearance is an ongoing process an estimation of a person's trustworthiness subject to ongoing evaluation over time a Facility Security Clearance is based upon factors which may change over the life of the clearance. After a facility has been cleared, a *changed condition survey* may be required when a change occurs that causes the information reported in the initial survey to be invalid. When the new survey is completed, the facility's status is re-evaluated.

A new survey is prompted when you report changed conditions to your DSS Field Office. You will recall that you need to make a report, for instance when there is a change in your firm's organization (such as a change of ownership) or a physical change (such as change of location).

Not all facility-related reports lead to a new survey. The DSS Field Office determines when a new survey is required. Your responsibility as the FSO in the matter is to file the report. The IS Rep will usually arrange a special trip to your facility, unless a security review has already been scheduled.

What the IS Rep needs to see during the visit is determined by the type of change you reported. If, for example, you reported a change of operating name, the IS Rep would examine the documentation of that change; Papers filed with

the state or local government, business licenses, board resolutions, etc.

GOVERNMENT INSPECTIONS REVIEWS

A government security review is a tool used to assess the effectiveness of the contractor's industrial security program and to assist you, the FSO in directing resources toward efficient and effective security solutions.

The security review, like the survey, is conducted by an IS Rep. If your facility is large enough to warrant it, more than one IS Rep may perform the security review. In some cases the security review may be completed over several months.

FREQUENCY

How often are government security reviews conducted at your facility? Security reviews are normally conducted once a year. Security reviews are conducted every 18 months at facilities that do not possess classified material. Events that may require DSS to conduct a security review in less than a 12 month period would include:

- New counterintelligence (CI) information that indicates a new or increased threat to the facility or its technologies
- Changes in the scope of the facility's classified operations
- User agency concerns
- Major or repeated security violations which indicate that classified information is not adequately protected
- Significant changes to FOCI
- Any new international involvement

NOTIFICATION

A government security review is normally *announced*. This means that as a courtesy, approximately 30 days prior to an announced security review, you will receive written notification from your IS Rep that your security program has been scheduled for review. You may also receive notification by telephone. You will be provided the date(s) of the upcoming security review.

This advanced notification gives you, as the FSO an opportunity to prepare for the security review. You should use this opportunity to ensure that management personnel will be available for discussion with the IS Rep and for the IS Re post-review briefing, and that other employees will be available for interviews. It is recommended that the FSO notifies all employees when a government security review is scheduled. You should also use this time to prepare a list of the classified contracts on which your facility is performing and to ensure that all records pertaining to the security program are available for review.

Unannounced security reviews are conducted by the IS Rep when specific concerns or problems occur at a facility.

NOTE: An IS Rep is considered a classified visitor. The Security Agreement coupled with the IS Rep's credentials and NISPOM paragraph 6-102, provide the authorization for the IS Rep to review your security program without having sent you a visit request.

WHAT IS AN INSPECTION LIKE?

In this section, we'll look at what the government security review of a non-possessing facility entails. The review is relatively simple for facilities that do not possess classified material. The IS Rep will normally be concerned with three basic areas: The status of the facility clearance, the status of personnel security clearances/access authorizations, and the level of security education and awareness at the facility.

The status of the facility security clearance (FCL)

The status of personnel security clearances (PCL)/
access authorizations

The level of security education and awareness at the facility

There might well be additional matters of interest, such as visit control. If the facility has prepared a written Standard Practice Procedures (SPP), the IS Rep will want to review it and see how it is implemented. Even the issue of safeguarding is a concern at facilities which formerly held classified information and are now dormant.

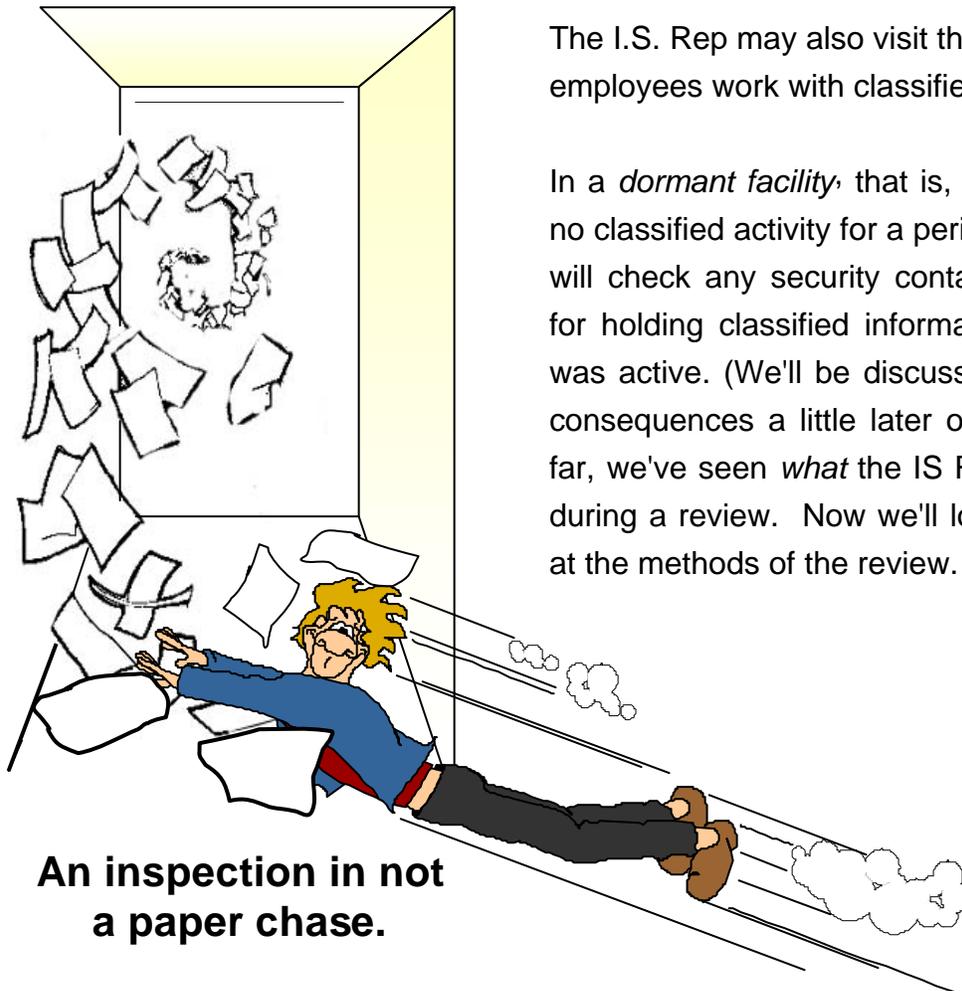
Let's look at the three basic concerns first. In determining the current status of the FCL, the IS Rep will look for any changes in the business structure and any changes affecting those personnel cleared in connection with the FCL (KMPs). The IS Rep will also be interested in whether or not any changes which have occurred have been properly reported. To determine changes in business structure, the IS Rep might look up a number of records, such as business licenses, articles of incorporation, minutes of meetings of the board of directors, minutes of stockholders meetings, and the most recent annual report. The IS Rep may look at any record(s) that tells something about the current status of the business. A knowledgeable official of your firm might be asked to review the Certificate Pertaining to Foreign Interests (SF 312), when applicable, to see if it is accurate and current and to determine any *anticipated* changes in this area.

In checking both the access authorizations and the level of security education, many factors may surface. For example, is there a true need for the clearances? Have all employees requiring clearances been granted them? Are employees holding unnecessary clearances or clearances at an inappropriate level? Have cleared employees been briefed, and are they aware of the security procedures involved in the performance of their duties? Questions of this type are best answered by the employees themselves. Security, after all, is not just a matter of paperwork. The basis for any security program is people, and in order to review your security program the IS Rep will be talking with people in your facility.

The subjects just covered (FCL, PCLs, and Security Education) form the core of any security review. Other areas are looked into as the situation demands. One of these areas almost certain to be addressed is *classified visits*. For a non-possessing facility the primary concern is outgoing visits. The I.S. Rep will be interested in any current visits and the system the FSO uses to keep track of the employees sent out. The IS Rep may also want to talk with some of the employees who have been out on classified visits. As indicated in the lesson on visits, the security responsibility rests with the host facility.

The I.S. Rep may also visit the location where the employees work with classified information.

In a *dormant facility*, that is, a facility that has had no classified activity for a period of time, the IS Rep will check any security containers that were used for holding classified information when the facility was active. (We'll be discussing dormancy and its consequences a little later on in this lesson.) So far, we've seen *what* the IS Rep will be looking for during a review. Now we'll look a bit more closely at the methods of the review.



**An inspection is not
a paper chase.**

INSPECTION TECHNIQUES

The IS Rep will arrive at your facility on the date specified in the letter. The IS Rep will first wish to make contact with you (the FSO) and senior management. During this initial get-together or entrance brief, the IS Rep will discuss the general plan of the review and solicit input from you and your management regarding any issues of security concern or areas of potential focus. In the review of a large facility that is heavily involved with the NISP, this stage is necessarily more complex and the planning of the review may, in fact, be done some days in advance.

While there are a certain number of areas to be reviewed, there is no set order of precedence in which they must be covered. This being the case, it is not possible to tell you, step-by-step, what will be looked at and who will be talked to, in any given order. We have, however, already gone over the items most commonly examined in the course of a review and can now discuss a little of the philosophy behind it.

After the initial meeting with you, the IS Rep will be involved in two types of activity, the *review of various records* and *interviewing personnel at your facility*. In order to gain an accurate picture of your security program, interviews of the employees are essential to the review process. If your facility possesses classified material, the review would take on a third dimension a concern with the physical security of the classified material. In all of these activities, you may wish to accompany the IS Rep personally or assign someone to accompany

him/her. While this is not required, it might serve as a training vehicle to you or your designee. It should be noted that the IS Rep may decide to conduct unaccompanied interviews. Certainly someone should be available to help in locating files and documents and to assist, should any problems arise.

RESULTS OF THE REVIEW

Upon completion of the review, the IS Rep will first brief you the FSO concerning the details of the review. Afterwards, a briefing is provided to senior management concerning the overall security posture of the company. The adequacy of security systems in place in your company will serve as the basis for the evaluation of the overall security posture. A rating of the security review will be assigned as follows:

Superior. A superior rating is the highest rating given to a contractor. A superior rating is given to contractors that have far exceeded the security requirements of the NISPOM when compared to other contractors of the same or similar size and complexity. This facility must have an outstanding security education program. Employee's must be fully aware of their individual security responsibilities, and demonstrate a cooperative spirit and awareness of security procedures. This rating also requires a sustained level of management support for the security program and the absence of any serious security issues.

Commendable: A commendable rating is given to contractors that have exceeded the basic security requirements of the NISPOM in one or more areas

of their security program, but do not meet the standards or level required to achieve a superior rating. Like the rating of superior, the contractor must have strong managerial support, minimal administrative findings, and the absence of any serious security issues.

Satisfactory: A satisfactory rating is the most common rating given to cleared contractors. A satisfactory rating indicates that a contractor's security program meets the basic requirements of the NISPOM. It indicates that there is minimal or no threat to the security of classified information at the cleared facility. This rating may be assigned even if there were administrative or isolated serious findings that require corrective actions.

Marginal: A marginal rating is given when serious findings are noted in one or more areas and these findings could lead to the loss or compromise of classified material if not corrected. The IS Rep will consider the size of the facility, extent of classified activity, and cause of the findings when giving a contractor a marginal rating. In addition, when a marginal rating is given, the IS Rep will normally schedule a compliance security review within 30 but no longer than 120 days.

Unsatisfactory: An Unsatisfactory rating is assigned when circumstances and conditions indicate that the facility has lost, or is in imminent danger of losing, its ability to adequately safeguard the classified information in its possession or to which it has access. This rating is appropriate when the security review indicates that the contractor's security program can no longer

preclude the disclosure of classified information to unauthorized persons.

The IS Rep will provide you a full explanation of the rationale for the assigned rating. The IS Rep will also advise you of any isolated individual failures or individual instances of non-compliance with a security requirement and will provide guidance to correct or resolve the issue. These types of issues will only be briefed to top management or included in the letter to top management if the individual or security system failure resulted in a compromise or suspected compromise or if a pattern has been identified which suggests the system is inadequate.

The IS Rep will almost certainly have found positive, even praiseworthy, facets of the security program, so this talk should provide an occasion for kudos as well. The FSO should feel free to make use of the IS Rep as a liaison between you and top management personnel. This will be an ideal time to raise important concerns/ issues about the security program that may have fallen on managers' deaf ears up to now. For instance, maybe the firm is winning more classified contracts than the FSO can properly monitor. The FSO may need an assistant to help with the workload. Tell the IS Rep. As an official representative of the U.S. Government, the IS Rep has considerable authority, and his/her voice added to yours on important issues may be just what's needed to convince management to take action.

EXIT BRIEFING

Once the IS Rep has briefed you, the FSO, the IS Rep will meet with senior management (assuming that you and senior management are not one and the same). During this exit briefing, the IS Rep will stress key issues regarding the facility's security program. The IS Rep will advise senior management of the overall security posture of the facility and explain the reason the rating was assigned. Remember, the IS Rep will only discuss instances of non-compliance with top management if a compromise or suspected compromise has occurred or the IS Rep has identified a pattern which suggests the system is inadequate. Even if there are no such problems, the exit briefing is still held to let management know what the overall security posture of the facility is and to brief them on any security topics of special interest, for example, an upcoming change to the NISPOM that affects your facility. And here again kudos from the IS Rep may be in order.

LETTER TO MANAGEMENT

Your facility's management will also be notified in writing of the results of the review. This letter will:

- Reiterate the security posture of the company.
- Highlight positive aspects.
- If appropriate, thank or commend members of the management or the security staff.
- Provide recommendations for security program improvements and stress areas of concern.

Again, this notification will only identify instances of non-compliance if a compromise or suspected

compromise has occurred or a pattern exists which suggests that the system is inadequate.

DSS FIELD OFFICE FOLLOW-UP

If the letter to management noted serious security problems, the DSS Field Office/IS Rep may conduct a special security review to determine that the problems have been corrected. Follow-up reviews are generally limited to determining and evaluating the correction of system failures.

UNSATISFACTORY RATING

The "worst-case" situation for the government security review is one where it is determined that the facility is unwilling or has consistently demonstrated an inadequacy to protect classified information. In this situation, the IS Rep may recommend to the DSS Field Office Chief revocation of the FCL Recommendation for revocation will be preceded by placing the facility in an *unsatisfactory* status and should be considered only when the contractor takes no effective action to improve their security posture. An unsatisfactory status indicates that the facility is no longer capable of protecting classified information and that revocation of the FCL is under consideration. An unsatisfactory rating is brought to the attention of the government customer(s). The Field Office may also advise these customers that the company should not be considered for any new classified work until conditions have improved. If management remains unwilling or unable to take effective corrective action, the facility's security clearance would be revoked. This is done only after a very careful review of the situation by highly-

placed, experienced NISP personnel. Fortunately, this is a very rare occurrence.

DORMANT FACILITIES

Finally, a review may reveal that a facility is dormant. A dormant facility is one that does not have active classified contracts, has not been afforded authorized access, and has no prospects for obtaining a classified contract. Unless something happens to end the facility's dormancy, DSS will administratively terminate the facility's clearance 24 months from the date of the facility's last access. The facility can be cleared "in an expeditious manner" if it again requires access.

FINAL SECURITY REVIEWS

A *final security review* is conducted when a possessing facility ends its involvement with the NISP. It may be that the contractor no longer wishes for whatever reason to perform on classified government contracts. It may be that a dormant facility's clearance is to be administratively terminated or that an unsatisfactory facility's clearance is to be revoked. Whatever the reason for conducting it, a final review is a formal review that includes other elements as well. These other elements terminate the cleared status of the facility. For example, the IS Rep will ensure that there is no classified information on site; that all cleared personnel have been (or will be) debriefed; that any outstanding classified visit authorizations have been cancelled, and that all security related files are in order. The IS Rep reviews with the FSO

which records must be maintained in the future and for how long.

SELF-INSPECTIONS

Self-inspections are conducted by you, the FSO. In the ongoing government-industry partnership, the day-to-day tasks of running a successful security program are carried out by the people at the industrial facility. While the DSS Field Office's review of the state of the company's security program is a useful evaluation tool, there is no way that the government, (IS Reps) can begin to carry out the role of overseer. The security program is ultimately the responsibility of the designated FSO. One of the best tools for monitoring and evaluating the program is the self-inspection.

FREQUENCY

You must review your security system on a continuing basis and conduct a formal self-inspection at intervals consistent with risk management principles. The word "intervals" gives you considerable latitude in deciding when to conduct a self-inspection. However, common sense should keep you from conducting it the day before or the day after a government review. It is recommended to conduct a self-inspection once a year or approximately six months following the DSS security review.

CONDUCTING A SELF-INSPECTION

You should model your self-inspection on the DSS review. The Defense Security Service Academy has prepared a guide to conducting self-

inspections for NISP contractors. *This guide, The Self Inspection Handbook for NISP Contractors* is available from your IS Rep. If your facility does not possess classified information, you will probably need to deal with only a few of its headings. The sections of the handbook on the following topics may apply to any cleared facility:

- Facility Clearance
- Access Authorizations
- Security Education
- Standard Practices Procedures
- Visit Control
- Foreign Ownership, Control, or Influence (FOCI)
- Consultants

The best way to use the *The Self Inspection Handbook for NISP Contractors* is to go down the list and ask yourself which questions apply to your facility, as well as the logical follow-ups to those questions. For example, if you're answering a question, which asks if a personnel clearance record is maintained, don't just locate the record. Read it carefully. Are there people listed who no longer require access? Does everyone listed still require access at the levels indicated?

Don't just go down the handbook's list at your desk if the question concerns the Security Agreement, locate the agreement. Like the IS Rep, you should do more than a mere paper check. It is the entire security system you are interested in, not just the related paperwork. Talk to the employees (you should be doing this on a regular basis, anyway). This needn't be a formal interrogation a friendly chat will suffice, if it gives you the information you're after.

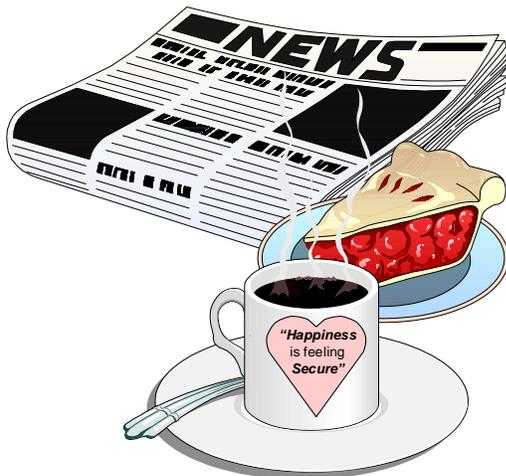
ANALYZE AND CORRECT

When you've finished your self-inspection, what then? Obviously, you should correct any problems that surface. Don't just leave it at that. Take a good look at *what caused the problem*. Was it a single, isolated incident or was it a symptom of a flaw in the security program? If your analysis shows that your procedures are inadequate or ineffective, revise them. The whole idea of the self-inspection is to give you, the FSO, a chance to review your security program *in its entirety*. Your review should ensure that your facility's overall security posture is adequate and that you are ready for the next Government Security Review.

AN EXAMPLE OF A SELF-INSPECTION

On the following pages we have provided a sample self-inspection conducted a short time ago at EWS by Harriet Hornsby, FSO. This is hardly an all-inclusive inspection, but it may at least give you a taste of what's involved.

SELF-INSPECTION AT EWS



As she did every morning at about twenty minutes to eight, Harriet positioned her coffee and cherry pie on the corner of her desk and spread the A.M. edition of the *Wombat Heights World Herald* out before her as she glanced at her current daily planner.

Oh, heck. She thumbed through her last year's daily planner and confirmed it. It was exactly one hundred and eighty-four days ago that George

Porgee, IS Rep, had been here at EWS for the government inspection. She realized that when George came by for his next inspection in a year or so, he wouldn't be particularly concerned about the exact timing of the self-inspection.

Putting away the paper, she turned to her copy of *The Self-Inspection Handbook for NISP Contractors*.

A. Facility Clearance.

1. Are the DD Forms 441 and/or 441-1 and SF 328 properly executed and maintained in a current status?



This being a branch office, Harriet knew that EWS needed the 441-1 and a copy of the 441 for EWC. Now where did Mr. Wilbersnoot keep those things? Then Harriet remembered. They are filed with the other legal documents in his personal safe. The one for which only he and his secretary, Wanda Fishtank, had the combination.

Mr. Wilbersnoot was away for a week, which meant Wanda would have to open the safe. Harriet was a little leery of asking her. Wanda was very protective of EWS, and of Mr. Wilbersnoot in particular. And Harriet felt as though Wanda had never quite forgiven her for the two weeks when she had replaced Harriet as FSO. Wanda blamed her in some way for this, although it had been Mr. Wilbersnoot's idea.

Fifteen minutes later, Harriet peered into the small crack Wanda had opened in the safe. Balancing her coffee mug on the edge, she used both hands

to open the drawer further. It took her another five minutes to find the 441-1. She made a mental note to have a talk with Mr. Wilbersnoot about his filing system.

Harriet was so happy to have finally gotten her hands on the 441-1 that she forgot all about her mug on the edge of the safe. After she mopped off the 441-1, she realized, to her horror, that it was now a sort of Mississippi River brown. Was it still a legal document? She could make out the signatures and she supposed the color of the form didn't matter. But what would she tell Mr. Wilbersnoot? Putting the 441-1 back in the drawer, she saw the copy of EWC's 441. She went to the next question.

2. Have all changes affecting the condition of the FCL been reported to the DSS Field Office?

The only changed condition reports lately were those reporting changes in KMPs. She'd filed a report with the DSS Field Office when Wanda had replaced her as FSO. And then Wanda had filed a report when Harriet took the job back.

3. Does the home office have an FCL at the same or higher level than any cleared facility within the Multiple Facility Organization?

Harriet was well aware of EWC's TOP SECRET facility clearance, which was at a higher level than the SECRET FCLs of both EWS and Electric Widget Distributors, the other branch office in the MFO.



4. Are the senior management official, the FSO and other Key Management Personnel cleared as required in connection with the FCL?

No one other than the FSO (Harriet) and senior management official (Mr. Wilbersnoot) had been required to be cleared in connection with the FCL. There were no uncleared officials who required exclusion at EWS, so she skipped question 5 and went on to question 6. Since there were no representatives of foreign interests at EWS, Harriet skipped question 6 too.

B. Access Authorizations.

1. Is a current record maintained of all cleared employees at each facility?

All that stuff was kept in the filing cabinet in the office that the Sales and Services people shared. Opening the bottom drawer, Harriet pulled out the list of EWS's cleared employees. There were only seven, and the list was current. Harriet didn't stop with the list, though. She checked the contents of the personnel security files. These files, arranged alphabetically, were kept on all currently cleared personnel. In each file, Harriet kept the LOC and a copy of all paperwork sent to the government (DISCO) regarding the person's clearance. There had been no changes, aside from Wanda's new clearance, since Porgee's last review, and all the paperwork appeared to be in good order.



Roberta Baloon

2. Is the number of clearances held to a minimum consistent with contractual requirements?

Harriet considered. She and Mr. Wilbersnoot had to be cleared as KMPs. Wanda had been cleared for her short-lived career as an FSO. Harriet put Wanda's folder aside. She would have to get that clearance terminated. The other clearances were for the three service personnel who did work on classified projects and one for a salesman who took part in classified contract negotiations. She decided to have a talk with the four to see if they still needed their clearances. Jimbo Duggins was out today on a classified visit. Duncan Undersides was next on her list. He was down in Supplies, refilling his repair kit, so Harriet turned to Roberta Baloon, the third of the cleared service personnel. Roberta was just on her way out when Harriet caught her. "Have you been out on any classified visits lately, Bobbie?"

"Not for some months now."

"Will you be going out on any in the future?"

"Not that I know of, but you know I'm cleared in case Jimbo needs assistance on the Air Force contract."

Harriet recalled the justification for Bobbie's clearance. Sometimes it took more than one person to do a repair job. It was a valid reason.

"Where's Slick?" Harriet asked Roberta, referring to the salesman who was cleared to negotiate classified contracts.

"I don't know and I don't care," snapped Roberta, "I haven't seen that snake since last Thursday."





SLICK GIBSON

Thursday was the day of the Great Sales and Services War. Tension had been building between the two sides for a week. Sales claimed that Services had an excessive amount of floor space for a group of people who were away most of the day. Services countered that Sales tied up the telephones from morning 'til night. At first just words were exchanged. Then things really got serious. Someone made a paper airplane out of a memo and sailed it at the opposing camp. Soon memos and directives and order forms were flying in all directions. When the combatants ran out of supplies, they requisitioned any loose paper they could get their hands on. Before the day was out, the floor was littered with crumpled aircraft. And EWS's filing system was in shambles.

Each side blamed the other, which was, in short, why Roberta Baloon and Slick Gibson were not on speaking terms.

Slick was over by the water cooler.

"Hi there, beautiful! How's security biz?"

Harriet sometimes wished she and Gibson weren't on speaking terms either.

"Have you taken part in any classified negotiations lately, Slick?"

"No, but I've got a hot contract in the works with NASA. It'll be the biggest thing this little company has ever seen. And real TOP SECRET stuff."

Slick was always talking like this, so Harriet made a note to ask Mr. Wilbersnoot about this "hot

contract." In the meantime, she spotted Duncan coming out of Supplies.

"Do you do work at any classified sites, Dunc?"

"Not at the moment, but the Air Force job is due in any day and more manpower is going to be needed."

She would call her contact at the Air Force to confirm that.

As it stood now, she had one unnecessary clearance and two which were perhaps questionable. The fewer clearances she had to keep up with, the better. She read through the remaining questions about access authorizations.

3. Has a Letter of Consent (LOC) been issued for each personnel clearance (PCL)?

Yes. She had found all seven LOCs in her files check.

4. Are all pre-employment clearance applications based on a written offer and acceptance of employment?

Yes. No one was put in for a clearance before being hired "on paper" first.

5. Are all required forms and information regarding cleared personnel furnished to DISCO?

She had kept copies of all DISCO Forms 562 and other information transmitted to DISCO. There



hadn't been anything to transmit to DISCO since the last government review. If Wanda's clearance was going to be terminated, however, Harriet would have to transmit a DISCO Form 562.

6. Are employees in process for security clearances informed of their options regarding completion of the privacy portion of the SF 86 application form?

After Harriet and Wanda completed the SF 86 in EPSQ for the SECRET clearance. (Harriet downloaded the software from the DSS website, www.dss.mil). She had a little trouble at first, but after she called the Support Services Center at 1-888-347-5213, she had no problems). Harriet had validated the information before transmitting it. Except for modules 17-42. Harriet had informed Wanda of her right to privacy regarding the information she provided in those modules. Wanda had masked that information by invoking a second password. Harriet had made sure that the information in the other modules of the SF 86 in EPSQ agreed with the information on the fingerprint card she placed in the envelope to DSS. She had done a very thorough job of it, and DSS had not called requesting additional information.

7. Has the contractor elected to have PCLs issued to the home office facility (HOF) or has an alternative arrangement been approved by the DSS Field Office?

The DSS Field Office had approved EWC's request to allow PCLs to be issued to its two branch offices, so EWS kept the seven LOCs for its cleared employees. Question 8 was about the same as 5,

except that it seemed to include reports on KMPs that went to the DSS Field Office. There weren't any of them.

C. Security Education.

1. Does the contractor provide all cleared employees with security training and briefings commensurate with their involvement with classified information?

All of the cleared personnel at EWS had received a comprehensive initial security briefing, and Harriet always gave refresher briefings at least annually. She found the information posted on the DSS web site very helpful in keeping her briefings interesting. (Last year the employees complained that she said the same thing every time). She kept each year's notes on file along with the employee sign-up sheet she passed around. The cleared personnel at EWS did not need NATO, CNWDI, or other special briefings.

2. Are contractors who employ cleared persons at other locations ensuring the required security training?

The service personnel performing work at Gizmo received special briefings on site that specifically addressed the project they were working on.

3. Are SF 312s properly executed by cleared employees prior to accessing classified and forwarded to DISCO for retention?

After each initial security briefing, Harriet had required the cleared employee to sign an SF 312. As a precaution, she had made a copy of the

signed form before she sent the original to DISCO. (After receiving Industrial Security Letter 95L-1, Harriet made sure that all those SF 312s executed after July 31, 1995 were forwarded to DISCO for retention).

NOTE: NISPOM Paragraph 3-105 requires that an individual issued an initial personnel security clearance (PCL) execute an SF-312, Classified Information Nondisclosure Agreement prior to being granted access to classified information, and that the facility submit the original SF-312 to DISCO for retention. **Please note this requirement applies only to individuals granted an initial PCL.** PCL's resulting from conversions or reinstatements should not be forwarded to DISCO.

4. Are refusals to execute the SF 312 reported to DISCO?

No one at EWS had ever refused to sign the SF 312.

Question 5 asked whether initial security briefings covered everything they were required to cover, and question 6 asked whether refresher training was given. She had already answered these.

5. Are cleared employees debriefed at the time of a PCL's termination, suspension, revocation, or FCL termination?

Harriet remembered giving the termination debriefing to Willona Riggs, a former cleared employee. Thank goodness she had never had to give a debriefing under other circumstances!

Questions 8 and 9 asked about EWS's reporting awareness procedures and the reporting procedures themselves. The EWS system was simple but effective: Harriet told and reminded all cleared employees to report required information to her, and she in turn made the formal reports to the proper governmental authority. Question 10 was about DSS providing special briefings and debriefings; it did not apply to EWS. Harriet checked with the EWC personnel office to see if there were any garnishments of pay at EWS. There weren't. She had asked Mr. Wilbersnoot if he was aware of any adverse information on EWS employees. He wasn't.

6. Has the contractor established a graduated scale of administrative disciplinary action to be applied against employees who violate the Manual?

Harriet and Mr. Wilbersnoot had set up such a scale. It started with a "verbal admonishment" and ended with dismissal. Harriet was proud that, as yet anyway, no cleared employee at EWS had ever violated the Manual. She thought there were two reasons for the perfect record. First, her training and awareness activities showed the employees the right way to do things, and second, the employees wanted to do things right....widget repair or security.

7. Are employees aware of the Defense Hotline?

Harriet had posted the information on the wall in the employee lounge area:

**The Defense Hotline
The Pentagon
Washington, D.C. 20301-1900
(800) 424-9098
(703) 604-8569
hotline@dodig.osd.mil**

8. Does management support the industrial security program?

Well, Mr. Wilbersnoot had always let Harriet do as she wished on security matters. He certainly seemed to understand the importance of it all, even if he didn't care much for the time it occasionally took up. She did, however, chat regularly with him and the other cleared employees about security matters and often pointed out to him interesting cases she found in the newspaper and other security awareness publications that Mr. Porgee sent her from time to time. She was never entirely sure that he listened.

EWS had no formal written Standard Practice Procedures, so she skipped that section, and the next section, subcontracting, was of no concern to EWS. This section was directed at firms that subcontracted out.

Down to **F. Visit Control** then

Most of this section was aimed at those contractors who received visitors, not those who sent them out. Questions one through four seemed to be the only ones directed at EWS.

1. Can the contractor determine that all classified visits require access to or disclosure of classified information?

The classified visits made by EWS were usually service calls that entailed the service person having access to classified information in the form of classified equipment. Harriet returned to the file cabinet. She pulled out the middle drawer and thumbed through her copies of recent VALs. While there was no requirement to keep copies of VALs, she always did so. This allowed the visitor to be located quickly if the need arose. Where was the copy of Jimbo Duggins' current visit letter? Well, she'd look for it later. Now she wanted to finish up the rest of the self-inspection.

2. Does notification of classified visits allow sufficient lead-time for the receiver's timely approval?

Harriet always sent out the visit requests as soon as she was aware of the need for a classified visit. That usually gave Gizmo at least two weeks notice.

3. Do Visit Authorization Letters (VALs) include the required information, and are they updated to reflect changes in the status of that information?

EWS's visits were service visits. The service people did not go to GIZMO to receive classified information from someone at GIZMO during the visit. So Harriet's VALs had never included a person visited other than the GIZMO FSO, Wellington Minor. They checked in with him and he took the visitor to the equipment needing repair

or maintenance. George Porgee had said this procedure was OK. She had never needed to update VAL information.

4. Are long term Visit Authorization Letters (VALs) updated as required?

EWS had no long term VALs in effect, so this question did not apply. Looking at the question started Harriet thinking, though. Maybe it would save paperwork to set up a long term VAL with GIZMO. She would talk with Jimbo, Roberta, and Mr. Wilbersnoot to find out whether they thought it was a good idea.



G. Classification.

Since EWS didn't actually possess classified materials, their concern in this area was limited to the guidance provided by the Air Force in the DD Form 254. The current DD 254 on file was quite adequate to the needs of EWS.

H. Employee Identification.

EWS was such a small operation, everyone knew everyone else, that there was no need for a badging or I.D. Card System.

Harriet skipped **I. Foreign Ownership, Control, or Influence.** Headquarters was responsible for FOCI matters, including updating the Certificate Pertaining to Foreign Interests.

J. Public Release.

EWS received quite enough business without having to advertise. And any yearly reports that were published came out of headquarters in New York. Harriet quickly moved on.

Because EWS didn't have any classified holdings, the next seven sections could be skipped. That brought Harriet down to:

R. Classified Meetings.

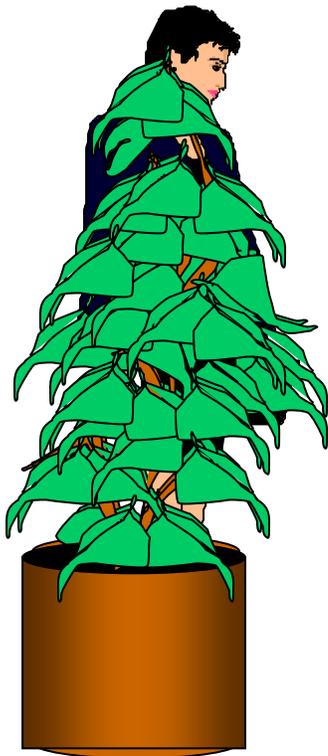
No problem, there hadn't been any.

She could pass over the sections on consultants, information systems for processing classified, and COMSEC/CRYPTO. EWS had none of that.

The next section of the handbook was **V. International Operations.** There had been talk of sending one of their service personnel to Canada to help out with a widget installation (not anything classified) but nothing had come of it. The last two sections of the handbook, OPSEC and special access programs, did not apply. Harriet was able to close her NISPOM with a smart snap, confident that she had completed a thorough self-inspection.

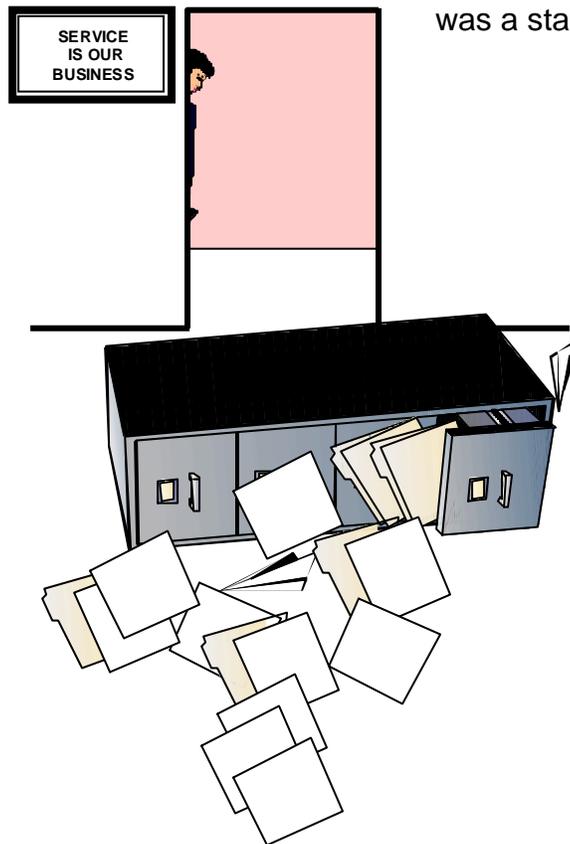
But where was that copy of the visit letter?

It had to be somewhere in the file cabinet. Harriet pulled out the top drawer. She leafed through the entire drawer of papers. No letter. Maybe it was in one of the large folders. She carried a folder back to her office. She had just reached her desk when a loud crack shattered the mid-morning silence. Suddenly she remembered why no one ever



opened all three drawers of the filing cabinet at the same time.

Wanda was looking at her accusingly when she came in to inspect the damage. The files had spilled out and slid across the linoleum all the way to the door, making a low-grade slope. The cabinet had crashed forward, closing all the drawers again. Only this time they opened to the bottom. Harriet noticed that a paper airplane had been trapped between the cabinet and the wall. A remnant, no doubt, of the Great Sales and Services War. She climbed across the files and picked it up. At least it was a start.



Two hours later, when everything had been refilled, Harriet remembered the paper airplane. Picking it up out of the trash can, she gave it a little celebratory flight. Before repositing it in the trash, she unfolded it. It was the missing copy of Jimbo Duggins' visit letter. Harriet sat back in her

chair and reviewed the morning's events. On the whole, not bad, she thought. Maybe she should rearrange the security files so that everything was in one drawer. The only real finding was Wanda's unnecessary clearance, and she would take care of that right away. Nothing seemed basically wrong with the system itself.

Then Harriet looked up. Wanda was staring at her from behind a large philodendron. "Oh dear," Harriet wondered, "am I going to have to submit my very first adverse information report?" It really did seem as if Wanda was behaving more strangely than usual.

SUMMARY

Surveys and reviews play a vital role in ensuring that classified information is properly safeguarded within the NISP. The Initial Facility Clearance Survey is a means of gathering information regarding a firm's suitability for an FCL. A changed condition survey may be required when information reported in the course of the initial survey is no longer valid. Security reviews are normally conducted on an annual basis and are normally announced. The review of a non-possessing (access elsewhere) facility usually addresses at least the three basic areas: the status of the Facility Security Clearance; the status of the Personnel Security Clearances (access authorizations), and the level of security education and awareness. Other areas are reviewed as appropriate. Records may be reviewed and employees will likely be interviewed. During an exit briefing with the facility's management, the IS Rep discusses the overall security rating, any system failures, and any problems requiring their attention to resolve. A letter to management formally notifies the facility of the review results. The Field Office may follow up with a special review. In extreme situations, when a facility's management cannot or will not protect classified information, an unsatisfactory rating is assigned. If such a situation remains uncorrected,

the facility's security clearance is revoked. When a possessing facility terminates its participation in the NISP, a close-out review is usually conducted. The FSO reviews the security system at the facility from day to day and conducts a self-inspection of the system at intervals consistent with risk management principles.

9 – Review Exercises

Complete the following exercises for review and practice.



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

1. List two "changed conditions" that may require a changed condition survey.

a. _____.

b. _____.

2. List three events that may cause DSS to conduct a security inspection of a facility in less than the normal 12 month period.

a. _____.

b. _____.

c. _____.

3. The review of facilities that do not possess classified information will usually address, as a minimum, the following three basic areas:

a. _____.

b. _____.

c. _____.

4. Another area that is usually covered during an inspection of a non-possessing facility is v_____ c_____.

5. The FSO will always receive a letter of notification of an upcoming government review several days before the date of the inspection.

() True. () False.

6. As for any classified visit, your facility will receive a visit request for the IS Rep's review.

() True. () False.

7. The IS Rep's review will usually consist of what two types of activity?

a. _____.

b. _____.

8. For each of the following, enter the type of rating awarded when the conditions described are encountered during a review.
- a. Rating: _____. Security Program meets the basic requirements of the NISPOM. Minimal system failures that are recognized and corrected before compromise have occurred; generally good knowledge among cleared employees of security procedures.
 - b. Rating: _____. Serious findings are noted in one or more areas, which could lead to inadequate protection of classified material. Management demonstrates no support for security or takes action that hinder security
 - c. Rating: _____. Contractor has exceeded the Basic Security Requirements of the NISPOM in many areas of their program, but do not meet the standards of a superior rating. Model security education program, top management actively supports maintaining an excellent security posture.
 - d. Rating: _____. This rating is assigned when circumstances and conditions indicate that the facility has lost, or is in imminent danger of losing, its ability to adequately safeguard the classified information in its possession or to which it has access. This rating is appropriate when the security review indicates that the contractor's security program can no longer preclude the disclosure of classified information to unauthorized persons.
9. Following the review, the IS Rep will provide you with a full explanation of the rationale for the assigned rating. The IS Rep will also advise you of any isolated individual f_____ or individual instances of n_____ with a security requirement and will provide g_____ to correct or resolve the issue.
10. The types of issues noted in item 9 will only be briefed to top management or included in the letter to top management if the individual or security system failure resulted in a c_____ or s_____ c_____ or if a p_____ has been identified which suggests the system is inadequate.

11. Specifically, the letter to top management will

- a. Reiterate the s_____ p_____ of the company
- b. Highlight p_____ aspects
- c. If appropriate, t_____ or c_____ members of the management or the security staff
- d. Stress areas of c_____, if appropriate.

12. An unsatisfactory status is assigned when a facility is _____

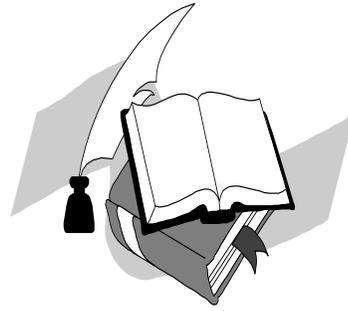
13. Your facility self-inspection must be conducted

- () a. immediately preceding government reviews.
- () b. once per month.
- () c. at intervals consistent with risk management principles.
- () d. every six months.

14. Desirable features of a facility self-inspection include:

- () a. locating and reviewing applicable documents, forms, correspondence and other paperwork.
- () b. talking to cleared personnel about any security problems you may have uncovered that relate to them and about any security difficulties they may be experiencing.
- () c. correcting any security problems you may have encountered.
- () d. analyzing the causes of the security problems that were identified and, where possible, eliminating the causes.

Solutions & References – 9



1. a. change in business structure/organization (e.g., change of name).
b. physical change (e.g., change of location).
(p. 9-3).
2. Any three of the events listed on p. 9-4 & 9-5. (p. 9-4 & 9-5).
3. a. The status of the Facility Security Clearance.
b. The status of the Personnel Security Clearances or access authorizations.
c. The level of security education and awareness.
(p. 9-6).
4. Visit control (outgoing classified visits). (p. 9-7 & 9-8).
5. False. (p. 9-5).
6. False. (p. 9-5).
7. a. Reviewing various records.
b. Interviewing personnel at your facility. (pp. 9-8 & 9-9).

- 8. a. Satisfactory
 - b. Marginal
 - c. Commendable
 - d. Unsatisfactory (p. 9-9, 9-10 & 9-11).

- 9. failure, non-compliance, guidance. (p. 9-11).

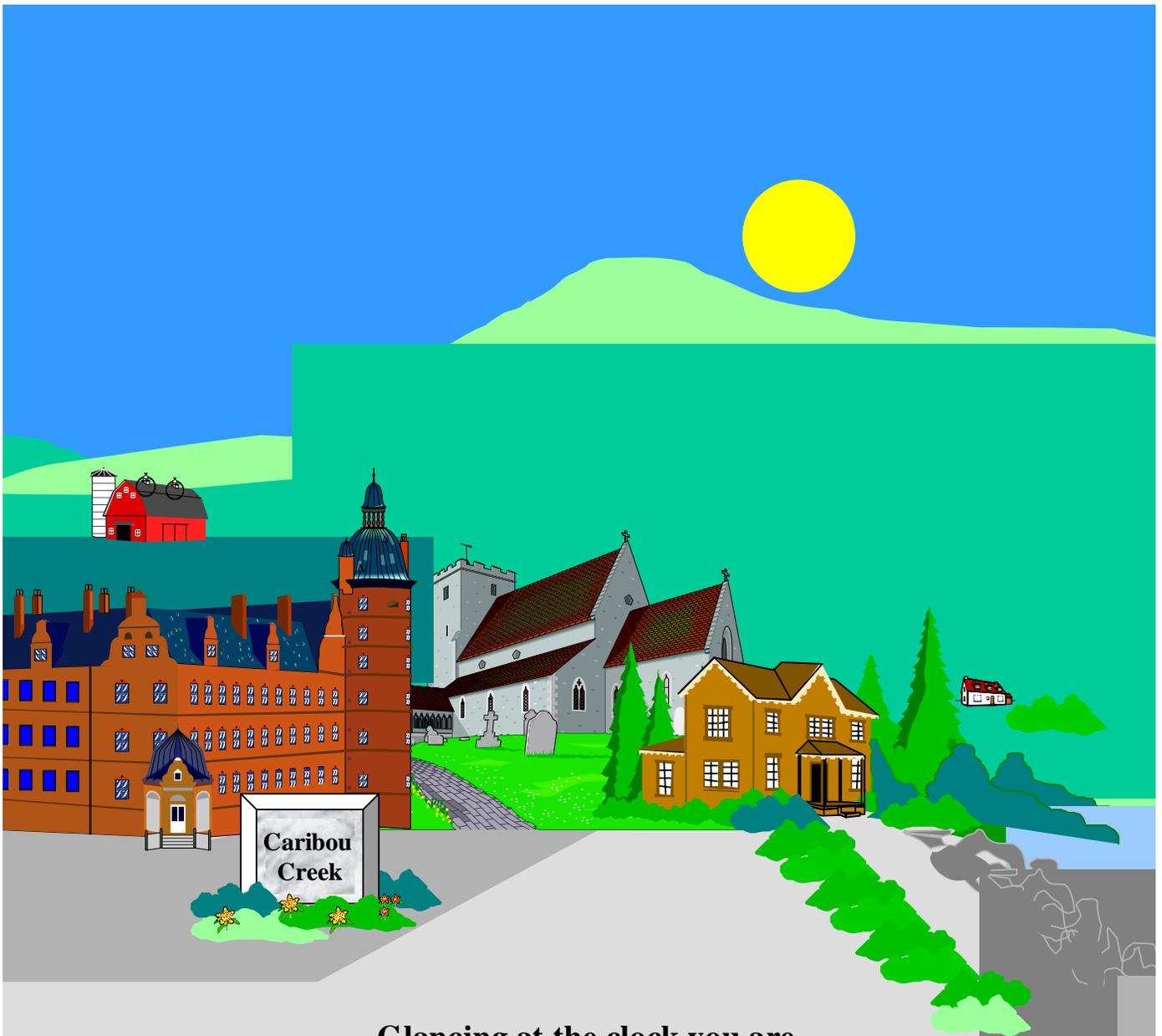
- 10. compromise, suspected compromise, pattern. (p. 9-11).

- 11. a. security posture.
 - b. positive.
 - c. thank, commend.
 - d. concern.
(p. 9-12).

- 12. cannot or will not adequately safeguard classified information. (p. 9-13).

- 13. c. (p. 9-15).

- 14. a, b, c, and d. (pp. 9-15 -17).



Glancing at the clock you are elated to discover it is time to go home! Fritz pokes his head in to tell you what a marvelous bit of work you have accomplished this first day on the job and to say that all the employees have been murmuring compliments about the new security officer. “I don’t know how you do it,” says Fritz, “but you’ve given us a morale boost for sure. We know we can count on you. See you tomorrow!! This job is going to be very rewarding, you feel, as you drive home. And the setting sun casts a warm glow over the little town of Caribou Creek.