

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.

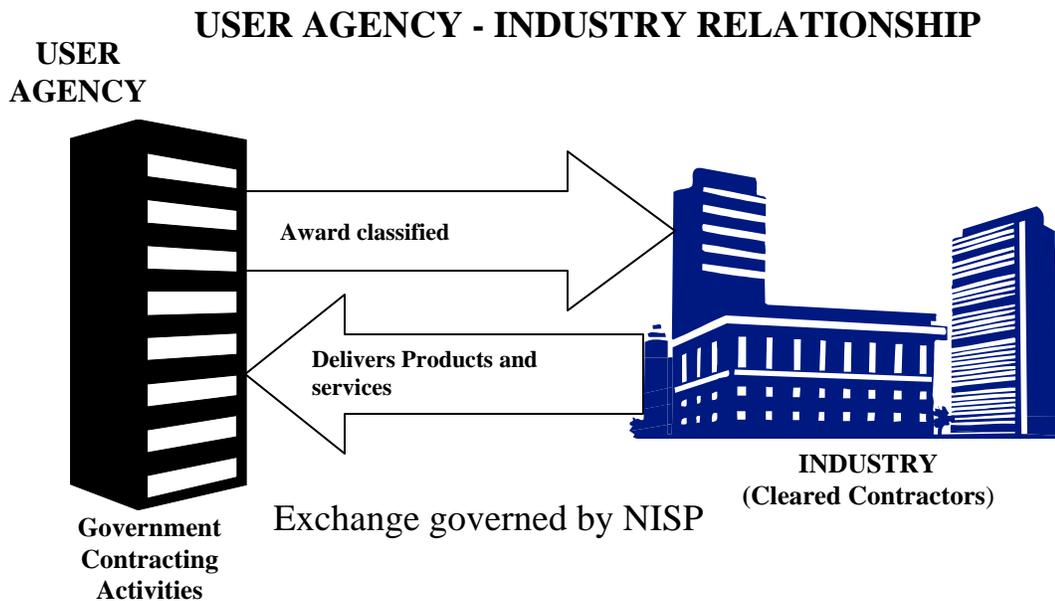
Each User Agency has one or more Government Contracting Activities (GCAs). *A GCA is an element of a federal department or agency that is designated to handle acquisitions for that department or agency.* Experts at GCAs of the User Agencies determine when one of their contracts will involve classified 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?

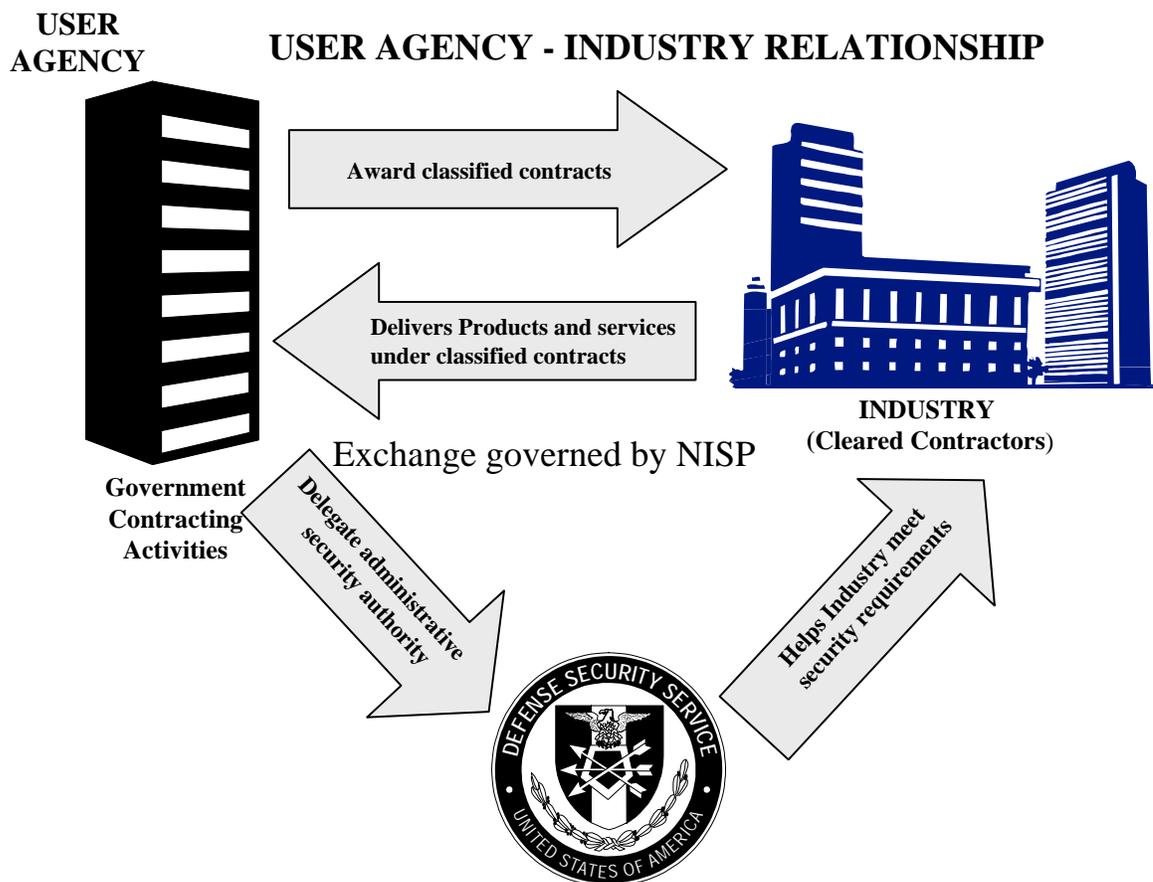
DEFENSE SECURITY SERVICE



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

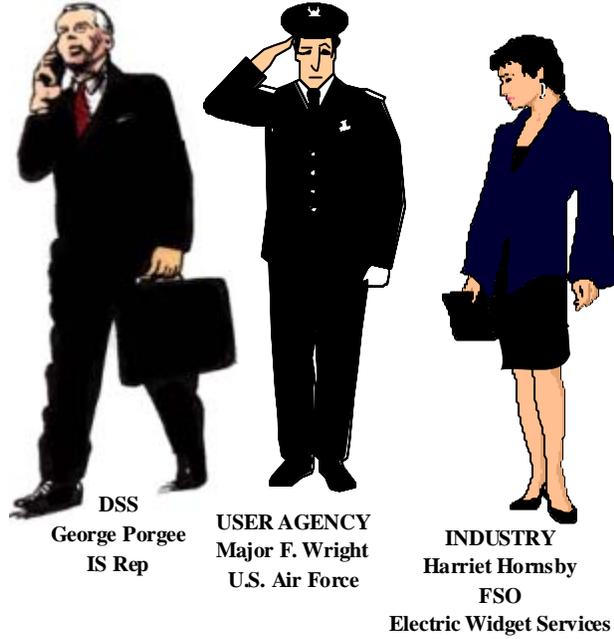


SUMMARY

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



DSS
George Porgee
IS Rep

USER AGENCY
Major F. Wright
U.S. Air Force

INDUSTRY
Harriet Hornsby
FSO
Electric Widget Services

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)