

LESSON 1

The Facility Security Clearance

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

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

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

OBJECTIVES

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

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

“FACILITY” DEFINED

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

THE FACILITY SECURITY CLEARANCE CONCEPT

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

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

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

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

FIVE ESSENTIAL ELEMENTS

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

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

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

SPONSORSHIP

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

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

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

There are thus three main considerations with sponsorship:

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

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

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

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

SECURITY AGREEMENT

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

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

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

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

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

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

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

CERTIFICATE PERTAINING TO FOREIGN INTERESTS

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

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

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

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

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

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

ORGANIZATION

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

THE PARENT-SUBSIDIARY RELATIONSHIP

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

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

THE MULTIPLE FACILITY ORGANIZATION

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

KEY MANAGEMENT PERSONNEL CLEARANCE

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

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

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

FACILITY SECURITY CLEARANCE NOTIFICATION LETTER

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

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

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

CHANGED CONDITIONS

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

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

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

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

REPROCESSING

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

FACILITIES ON USER AGENCY INSTALLATIONS

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

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

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

SUMMARY

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

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

REVIEW EXERCISES

Complete the following exercises for review and practice.

1. A facility security clearance is an administrative determination made by the Industrial Security Representative. The FCL is issued by the Defense Industrial Security Clearance Office.
2. Access is defined within the NISP as "the ability and opportunity to obtain knowledge of classified information."

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

True
False

ANSWERS

Solutions and References

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