

Process for Obtaining a DoD Facility Clearance

L. Bjerke¹

Holder Consulting Group, Renton, WA 98059, USA

This paper presents a brief overview of activities required to obtain a facility security clearance to allow your company to perform on classified contracts, and recommends an approach to expediting the process. Holder Consulting Group has experience in obtaining and managing the security clearance process, which can be long and tedious. However, it can be expedited by becoming familiar with the requirements and preparing needed materials ahead of time.

Nomenclature

<i>CAGE</i>	=	Commercial and Government Entity
<i>CCR</i>	=	Central Contractor Registration
<i>DISCO</i>	=	Defense Industrial Security Clearance Office
<i>DoD</i>	=	Department of Defense
<i>DSS</i>	=	Defense Security Service
<i>DUNS</i>	=	Data Universal Numbering System
<i>e-QIP</i>	=	Electronic Questionnaire for Investigation Processing
<i>FCL</i>	=	Facility Clearance
<i>FSO</i>	=	Facility Security Officer
<i>ISFD</i>	=	Industrial Security Facility Database
<i>ISR</i>	=	Industrial Security Representative
<i>JPAS</i>	=	Joint Personnel Adjudication System
<i>KMP</i>	=	Key Management Personnel
<i>NDA</i>	=	Non-Disclosure Agreement
<i>NISP</i>	=	National Industrial Security Program
<i>NISPOM</i>	=	National Industrial Security Program Operating Manual
<i>OPM</i>	=	Office of Personnel Management
<i>PCL</i>	=	Personnel Clearances
<i>POC</i>	=	Point of Contact
<i>SCI</i>	=	Sensitive Compartmented Information
<i>SPP</i>	=	Security Policies and Procedures
<i>TIN</i>	=	Taxpayer Identification Number

I. Introduction

A facility clearance (FCL), which is required in order to execute classified work for the US Department of Defense (DoD), is “an administrative determination that a facility is eligible for access to classified information or award of a classified contract”. Classification levels include Confidential, Secret, and Top Secret. The level of clearance your company is granted will be determined by the level indicated in the contract or subcontract you have been awarded. Requirements for obtaining an FCL include the following:

1. Access to classified information is required in performance of contract work;
2. Your company is located in the US or a US territory;
3. Due diligence will show that your company and all officers have participated in no unlawful activity and are not barred from working with the Government; and
4. Your company is not under foreign ownership, control, or influence.

¹ All rights reserved; express permission given to redistribute in unaltered form

The process for obtaining a facility clearance involves many steps, and attention to detail is very important. It may be tempting to rush through and short-cut steps to speed the process; however, it is important to let the process work as required. The DSS (Defense Security Service) expedites requests for both the facility clearance and associated personnel clearances, but each step requires review and/or adjudication. Brief instructions on obtaining a facility clearance can be found on the DSS website, but there are many additional details not included. This document is meant to provide an overview of the process.

No company is allowed to obtain a facility clearance unless a need has been specified by a government agency or by another company holding a clearance and requesting your company provide subcontracting services on a classified contract. Also, if your company is qualified to bid on a program that requires a classified proposal, the Government sponsor may request your company be granted a facility clearance. To perform on a classified contract, your company must have received a Form DD254 (Contract Security Classification Specification) from the agency or other company wanting your support. The DD254 indicates Government agency, contractor name, type of information to which access is required, activities required, security guidance, dates and number of contract, and certifying official, and defines the need for a facility clearance.

Facility security clearances may be granted at the Top Secret, Secret, or Confidential level. Storage of information also may be granted at a level equal to or lower than the facility clearance. Additional requirements pertain if your company will support programs requiring access to Special Compartmented Information (SCI). Those requirements are not addressed in this document.

II. Getting Started

Before beginning the FCL process, you will need your Taxpayer Identification Number (TIN) and a DUNS (Data Universal Numbering System) number. The DUNS system is copyrighted by Dunn and Bradstreet to identify each company's business location. After receiving your DUNS number, your company also must register at the Central Contractor Registration (CCR). This process will provide your company with a CAGE (Commercial and Government Entity) Code, which you will need for the facility clearance process.

Your company cannot submit the request letter to DSS for the facility clearance; it must come from your sponsoring agency or company. To expedite, as well as to assure all information about your company is correct, the best option for you is to prepare the letter and send to your sponsor for forwarding to DSS.

Once the sponsor's request letter is received by DSS, the process for your facility clearance will begin. After a period of time (possibly as long as a few months), you will receive a letter from the FCL Branch welcoming you to the National Industrial Security Program (NISP). Your account will be assigned to an Industrial Security Representative (ISR), who will help you through the entire facility and personnel clearance processes.

III. Preparation for Industrial Security Representative

Your ISR will contact you for additional information about your company that will help him/her determine specific requirements for your facility clearance. You should collect as much of this information and supporting documentation ahead of time so you can expedite your response.

Information you will be asked to provide includes the type of incorporation or ownership, any parent company, articles of incorporation, company by-laws, and agreements. Your ISR may ask you to also provide stock records and minutes of board meetings. Additionally, you will need to provide information on the percentage of ownership for each officer and the Chairman of the Board. Prepare a short summary of your company's business and products or services, company contact information (POC email and fax), and company locations for the past 10 years. Also be prepared to provide proof of US Citizenship for the person who will be your company's Facility Security Officer (FSO). The ISR will use all the information to understand ownership and operations of the company. He/she will then identify which officers will be required to have personnel security clearances coincident with the facility clearance. If you have a website, be prepared to provide your web address as well. This will help the ISR to advise you on protecting potential vulnerabilities to your company.

Your ISR also will send several forms to you that you and your company officers will need to complete and return. Instructions for each will be sent as well. These include:

1. Form DD 441, Department of Defense Security Agreement, Appendix C. This is an agreement between your company and the Government stating that a system of security will be set up to safeguard classified information. If your company has multiple facilities that will be included in the security agreement, a supplemental form, DD 441-1, also will be required.
2. Form SF 328, Certificate Pertaining to Foreign Interests, with which one of your corporate officers will declare any foreign ownership or influence for your company.
3. List of Key Management Personnel, which will provide personal information for the FSO and each of the company officers required by your ISR.

IV. Submitting for Personnel Clearances

The company's Key Management Personnel (KMP) must be cleared at the same level as the facility clearance level requested. Clearance processing for the KMP will be expedited because each one must be approved prior to being granted the facility clearance.

Individual personnel clearance (PCL) applications must be submitted to Defense Industrial Security Clearance Office (DISCO) using their online process. It may take quite some time for each individual to gather the necessary information, so it is best to begin preparations for submitting for individual personnel clearances, for at least the individuals most likely to be included in the KMP list, prior to receiving a notice that the process has been initiated. Each person should collect his/her background information, such as past residences, past employment, contact information for relatives, etc.

Once your ISR provides the KMP list to the DSS facility clearance branch, DSS will begin PCL processing on the required individuals (some may already hold clearances at the appropriate level under another organization and a new application will not be required). DISCO will initiate an electronic Questionnaire for Investigations Processing (e-QIP) for each of the required persons. Your ISR will contact you to provide instructions for completing the security questionnaires and guidelines on what to expect during the process. You will need to provide a copy of the instructions to each individual to complete his/her questionnaire.

Before each KMP submits the completed e-QIP form, the information must be printed out and provided to the FSO for review. This includes the personal questions in the second half of the questionnaire. The FSO position is one of trust and each person needs to be reassured of the FSO's integrity and that the information provided will be maintained as confidential. However, it is a requirement from DISCO that all information be reviewed for completeness prior to final submission.

You also will receive fingerprint cards that must be completed for each person. You will need to arrange with your local police department or a private authorized fingerprinting company to have these executed for each KMP. You should accompany each person to witness the fingerprints are valid for each one. Be sure to use the fingerprint cards sent by DSS, as only those will be accepted by the clearance office. If you do not receive enough cards, you can request more from DSS.

Once you have been notified that the Office of Personnel Management (OPM) has initiated the e-QIP process, individuals will have 30 days to begin entering data. It's important that each person logs on and enters at least the personal identification information. If not started within 30 days, the request will be cancelled and you will have to ask your ISR to reinitiate. The entire process must be completed within 90 days of initiation. You also must FAX to DISCO the release forms for each individual. The processing will not begin until that is received from you.

DISCO will need to review the e-QIP responses from the KMPs for any issues before granting an interim FCL. The turnaround time for the interim FCL varies from a few days to several weeks. It is OK to check status with your ISR and/or DISCO during this process, but you should not do so often. The final FCL determination will take longer. Investigations will need to be completed by the OPM for each KMP and the results are sent to DISCO for final adjudication. All the KMPs then must be granted final PCLs before the final FCL is granted. You should allow a year for final PCLs to be granted.

V. Briefing Personnel

Once you have submitted for the personnel clearances, you should start preparing to provide security briefings for the KMPs. The briefing will include threat awareness, defensive security, an overview of the security classification system, employee reporting obligations and requirements, and security procedures and duties applicable to the employees' jobs at your company.

The briefing may be written or in presentation form. However, a presentation is best, especially if this will be the first time for clearances for your people, as this will allow discussion of anything that might need further clarification. It is a good idea to have a form prepared for employees to sign acknowledging receipt of the briefing and agreement to abide by the rules and processes defined.

Employees also will need to sign a Classified Information Non-Disclosure Agreement (NDA), which is a contract with the US Government to protect classified information. It explains the executive orders that apply and laws covering the agreement, and defines penalties for violation of the contract. The employees will sign the agreement, another cleared person will witness the signature, and you, as FSO, will sign to accept the agreement. Following this, you may grant access to each person and they may begin working with classified information.

Your ISR will send you paperwork to complete and fax back to the DSS Security Call Center for access to the Joint Personnel Adjudication System (JPAS) system. This will allow you to view, check status, and manage clearance information for cleared people at your company. The form also provides for requesting Industrial Security Facility Database (ISFD) information to verify your company's information and to view facility information and points of contact for other companies. The form needs to be completed, signed by a company officer, and faxed to the DSS organization, along with a JPAS Account Manager Appointment Letter signed by the same nominating officer of your company.

VI. Preparing for Initial Inspection

Soon after receiving your interim FCL, your ISR will schedule a visit to your company for the initial security inspection. That visit will usually take place within a month of the contact, so you should begin preparation of much of your materials as soon as you submit for personnel clearances. You will need to have the following:

1. A documentation of your company's Security Policies and Procedures (SPP). You can obtain information on what is required for this from the NISPOM (National Industrial Security Program Operations Manual). You should download and become familiar with all sections of the NISPOM. Your SPP should include a summary of all the requirements presented in the NISPOM, with specifics of how your company implements the requirements. It also should include a diagram of your facility indicating where classified work may be performed, where data are stored, how to transport classified materials within your company (as well as externally), and any special precautions that must be taken to protect the materials.
2. If you are required to store classified data, you must have a Class 5 or Class 6 rated GSA (General Services Administration) approved cabinet. Every GSA Approved Container and cabinet must have a lock (digital or mechanical) that meets the Federal Requirements listed under Federal Specification FF-L-2740. Currently the standard for most of these containers is the digital X-09 lock that is designed to allow for either a single or dual combination for two-person integrity. Every GSA container approved for classified use will need to have an "Open / Closed" sign for each drawer, as well as a Security Container Check Record that will need to be initials with date/time each time the drawer is opened, closed, and checked. You should have these ready for your inspection.
3. To destroy classified documents, you will need an approved shredder. Your shredder must meet requirements of NSA/CSS 02-01, shredding to a size of 1mm x 4.7mm in size.

Your initial security inspection will include a check of the facility to assure it meets NISPOM requirements. You will need to provide a copy of the letter granting your company a security clearance, a copy of your KMP list, a list of your classified contracts, copies of the Forms DD254 for each one, and a list of your cleared personnel. Your ISR may recommend modifications to your plans for working with classified materials (such as closing blinds, locking doors, etc.), depending on your facility's layout and proximity to unclassified areas. He/she also will provide you with documentation, reference sources, and points of contact to provide you help and support as you manage your facility and personnel clearances.

If you will require the ability to access or generate classified documents on a computer, the computer will need to be approved for use in a classified environment and you will need to prepare a separate procedures document for its use. Instructions for this will be provided by your ISR representative during your facility clearance process. Requirements for setup and operation of the AIS (Automated Information System) can be found in the NISPOM.

VII. After the Inspection

DSS will continue to complete the background investigations of all KMPs. The process should be completed within about a year from initial submission. You can call DISCO to check after the year has passed. Once all KMPs have been approved for final PCLs, you will receive a second letter indicating your facility clearance is final. At any time after receiving your interim FCL, you may initiate e-QIP requests for clearances for additional employees.

VIII. Summary

The process for obtaining a facility security clearance to allow your company to perform on classified contracts can be long and tedious. The process, however, can be expedited by becoming familiar with all the requirements and preparing materials ahead of time. The most important activity is to read and understand the requirements provided in the NISPOM. Thereafter, as soon as each step in the process is completed, items for the next step should be prepared so everything is available quickly after it is request. That will reduce the time required for the FCL process to the shortest possible.

This paper presents a brief overview of the activities required to obtain a facility security clearance, and recommends an approach to expediting the process. Holder Consulting Group has experience in obtaining and managing the security clearance process.