A GUIDE FOR NEW FACILITIES

WELCOME TO THE NISP

The Defense Security Service (DSS) has received a request from either a Government Contracting Activity (GCA) or a cleared contractor to sponsor your facility for a Facility Clearance (FCL) in the National Industrial Security Program (NISP). The NISP was established by Executive Order 12829 in January of 1993 for the protection of classified information. The NISP applies to all executive branch departments and agencies, and to all cleared contractor facilities located within the United States, its Trust Territories and possessions. Participation is voluntary, but access to classified information will not be permitted otherwise.

When your facility receives its FCL, it will be subject to provisions of the National Industrial Security Program Operating Manual, usually referred to as the NISPOM. (The NISPOM may be downloaded from the DSS web site at http://www.dss.mil). This guide is not intended to replace the NISPOM, and your first order of business should be to review the NISPOM itself.

OVERVIEW

A facility is a plant, laboratory, office, college, university, or commercial structure with associated warehouses, storage areas, utilities, and components, that, when related by function and location, form an operating entity. (A business or educational organization may consist of one or more facilities as defined herein.) For purposes of industrial security, the term does not include Government installations.

The NISPOM describes a facility clearance as "an administrative determination that a facility is eligible for access to classified information or award of a classified contract." The FCL is valid for access to classified information at the same, or lower, classification level as the FCL.

The classification levels in the NISP are CONFIDENTIAL, SECRET, and TOP SECRET. The FCL level your facility receives is based upon the classified contract you have been awarded and its requirements. Interim clearances, based upon lesser investigative requirements, may be issued at each of these levels. An Interim FCL may be granted under certain conditions if your facility qualifies.

A facility must meet certain eligibility requirements in order to be processed for an FCL. As noted above, your facility must need access to classified information in connection with a legitimate U.S. Government or foreign requirement. The contractor must be organized and existing under the laws of any of the fifty states, the District of Columbia or Puerto Rico, and be located in the U.S. and its territorial areas or possessions. Your facility must have a reputation for integrity and lawful conduct in its business dealings, and your facility cannot be barred from participating in U. S. Government contracts. Finally, your facility must not be under foreign ownership, control or influence (FOCI) to such a degree that the granting of an FCL would be inconsistent with the national interest.

The Defense Security Service (DSS) has been delegated security administration responsibilities on behalf of the Department of Defense (DoD), and as such will advise and assist your facility during the FCL process. Your facility will be required, at a minimum, to execute certain designated forms, such as the Department of Defense Security Agreement, DD Form 441 (or DD Form 441-1 for certain facilities); process Key Management Personnel (KMP) for personnel security clearances; and appoint a U.S. citizen employee as the Facility Security Officer (FSO).

e-FCL

Your facility will be required to use the DSS Electronic Facility Clearance (e-FCL) online database to submit all applicable facility documents. The DSS Facility Clearance Branch registers all facilities for an e-FCL account. You will receive an automated notification when your facility has been successfully registered in the system. The e-FCL Contractor User Guide can be located on the DSS website at http://www.dss.mil/diss/efcl.html

FACILITY SURVEY

An IS Rep will contact you via telephone or email to schedule an on-site survey. This is the initial step in this process. The FCL survey is a detailed inquiry conducted to ascertain the type of business, the ownership and management of your facility, and any FOCI that may be present.

The facility clearance survey is conducted by an IS Rep of DSS. The IS Rep will assist your facility with the clearance process, provide you with an overview of the NISP and how your facility fits into the picture, and help you identify which KMP at your facility must be cleared.

To expedite the survey, it will be helpful if you have all relevant documents available (e.g., articles of incorporation, by-laws, partnership agreement, operating agreement, joint venture agreement, etc.). Some of these documents you may need to obtain from your facilities' legal counsel. It will be helpful if your KMP are available. Your IS Rep will be available for questions and to provide advice and assistance, and will conduct a periodic vulnerability assessment after your facility FCL is issued to help your facility maintain a strong and effective security posture.

CAGE CODE

It will be necessary for your facility to obtain a Commercial and Government Entity (CAGE) code if it does not already have one. CAGE Codes are completely separate and distinct from facility security clearances, but DSS uses CAGE Codes to track basic facility information. Your facility must be assigned a permanent CAGE Code by the Defense Logistics Agency (DLA) before it can be cleared.

If your facility does not already have a CAGE Code for the facility requiring clearance, one may be obtained by registering with the System for Award Management (SAM) database to get a CAGE Code at www.sam.gov. A guide on how to register in SAM can be found at: https://www.sam.gov/sam/transcript/Quick_Guide_for_Contract_Registrations_v1.7.pdf

SAM is the preferred method for obtaining CAGE codes. We recommend a search at the SAM site prior to requesting a CAGE Code to see if a CAGE Code may already have been assigned to your site.

Alternatively, submitting a DD Form 2051 to Commander, Defense Logistics Services Center, ATTN: DLSC-SBB, Federal Center, 74 North Washington, Battle Creek, MI 49017-3084. The DD Form 2051 can be found at: http://www.dtic.mil/whs/directives/infomgt/forms/eforms/dd2051.pdf

Section A of the form must be filled out and signed by the sponsoring government agency. Your sponsoring government agency may also request the CAGE Code for you by submitting a request on agency letterhead to the above address.

PARENT FACILITIES

If your facility is a subsidiary of another corporation, your parent facility (and all grandparent facilities) will need to be excluded from access to the classified information that is about to be made available to your facility. Your IS Rep will need to know complete identifying information about these parent facilities, to include: addresses, points of contact, and telephone numbers/email address. Your IS Rep will provide you instruction as to how these facilities will be processed as Excluded Parents in the NISP.

HOME OFFICES

If your facility is a branch or division of a Home Office facility, that Home Office will also need an FCL at the same or higher level as your facility. If your Home office facility is already cleared in the NISP, your facility will be included under the umbrella of your Home Office's Security Agreement and your facilities' FCL will be formalized on the DD Form 441-1.

If your Home Office facility does not have an FCL, it will need to be cleared. Again, your IS Rep will need complete identifying information.

e-QIP INFORMATION

It will be necessary for your facility to submit Personnel Security Clearance Applications using the Electronic Questionnaire for Investigations Processing (e-QIP) secure website. Failure to submit the required documentation in a timely manner could lead to the discontinuance of the FCL process for your facility.

DSS will assist your facility during the FCL process with the submission of all required Personnel Security Clearance Applications. DSS will only assist your facility for the initial processing of designated KMPs of your facility and may not be used for rank and file employees nor after your FCL has been issued. Any question about these procedures should be referred to your IS Rep.

JPAS INFORMATION

The Joint Personnel Adjudication System (JPAS) is the Department of Defense (DoD) database of record for personnel security clearances (PCL). JPAS provides "real time" information regarding PCLs, both investigative status and access eligibility, to authorized DoD security personnel and other interfacing organizations, such as cleared defense industry. Your customers in defense industry and in the Department of Defense will use JPAS to verify your PCL information.

Facilities must receive access to JPAS in order to maintain electronic PCL records. The requirements for registering for access to JPAS are that your facility must be in-process for a FCL, and that the employee who is going to be your Primary Account Manager in JPAS must have at least an Interim Secret Eligibility and an opened National Agency Check/Local Agency Check with a Credit Check (NACLC) investigation or Single Scope Background Investigation (SSBI).

JPAS ACCOUNT

To request a new JPAS account, you will need to submit a PSSAR DD Form X645, Letter of Appointment, and a copy of certificates of completion for both the Cyber Security Awareness Challenge/Security training as well as one of the Personally Identifiable Information courses. First, create a Letter of Appointment (LOA) on your facility's letterhead designating a Primary Account Manager. You may elect to also designate an Alternate Account Manager in the Letter of Appointment. Remember, these individuals must have at least Interim Secret Eligibilities with open investigations. A Corporate Officer or Key Management Personnel (KMP) listed in Industrial Security Facilities Database (ISFD) must sign the letter. One LOA may be created for multiple applicants within the same company if they share common job duties that require JPAS access. Second, a JPAS PSSAR form must be completed, signed, and submitted. The PSSAR form must be completed, signed, and submitted. The signatures need to be your Corporate Officer, your Security Officer, and the applicant.

For a complete guide on obtaining a JPAS account, access the Defense Manpower Data Center (DMDC) Website at: https://www.dmdc.osd.mil/psawebdocs/docRequest//filePathNm=PSA/appId=560/app_key_id=1559jsow24d/siteId=7/ediPnId=0/userId=public/fileNm=JPAS_Account.pdf

To obtain this form, access the Defense Manpower Data Center (DMDC) Website at: https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=JPAS . Then click on the link "Prospective SAR" to download the form.

Upon completion of the Access Request Form, the Letter of Appointment, and required courses, submit the documents to the DMDC Contact Center. The DMDC Contact Center FAX number is COMM (502) 613-1096, email address dmdc.contactcenter@mail.mil. Once the accounts have been created, the DMDC will notify you with your account information.

For new facility accounts, DMDC will create the account for the Primary or Alternate Account Managers. If your facility/organization already has a JPAS account at a different location, then you will need to contact the established JPAS Account Manager or JPAS POC within your company, as that Account Manager (for that other location) can create your account. Until your account is created, another authorized JPAS user in your company (with the appropriate access) should maintain your PCL records.

REQUIRED PKI/ SMARTCARD

DMDC requires all JPAS users to logon using DoD-approved Public Key Infrastructure (PKI) based logon credentials. A new JPAS user must meet the JPAS account requirements, submit a signed Personnel Security System Access Request (PSSAR) Form to their Service or Agency, and be approved to receive a JPAS account prior to obtaining DoD-approved Public Key Infrastructure (PKI). Instructions to obtain PKI can be found at:

• DMDC JPAS Documentation web site https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=JPAS , with the latest JPAS PKI FAQs posted in the left-hand column Refer to Section 2 (Question #29) and Section 4 of the JPAS PKI FAQs document.

• DISA's ECA PKI web site: http://iase.disa.mil/pki/eca/ for a listing of ECA PKI providers.

• DISA's Public Key Infrastructure and Enabling Website: http://iase.disa.mil/pki-pke/index.html .

The Secure Web Fingerprint Transmission (SWFT) program

Effective January 1, 2014, cleared companies listed in the Industrial Security Facilities Database will be required to submit electronic fingerprint files to the Defense Manpower Data Center (DMDC) for National Industrial Security Program (NISP) applicants. The Secure Web Fingerprint Transmission (SWFT) program enables cleared Defense industry users to submit electronic fingerprints (e-fingerprints) and demographic information for applicants who require an investigation by the Office of Personnel Management (OPM) for a personnel security clearance. Cleared contractors collect and securely transmit e-fingerprints to SWFT for subsequent release to OPM based on a JPAS/e-QIP submission approved by the Personnel Security Management Office (PSMO-I). Paper-based capture, submission and processing of fingerprints was time consuming and prone to errors. The SWFT eliminates the manual paper process, expedites the clearance process, and provides end-to-end accountability for PII data.

DSS has issued an Electronic Fingerprint Capture Options for Industry Guide at: e-fingerprints-DSS Guide

For a complete guide on obtaining an SWFT account, access the Defense Manpower Data Center (DMDC) Website at: https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=SWFT

ASSISTANCE

Should you need assistance during the clearance process or after your facility has been cleared, your IS Rep is your first point of contact. You can also obtain assistance through the DSS Customer Call Center at 1-(888)-282-7682 or contact Facility Clearance Branch at occ.facilities@dss.mil.