Defense Counterintelligence and Security Agency

Critical Technology Protection

Facility Clearance (FCL) Orientation Handbook

March 2021

Contents

Welcome Message

On behalf of the Defense Counterintelligence and Security Agency (DCSA), welcome to the first step in the Facility Clearance (FCL) process. DCSA is delegated security administration responsibilities and is the Cognizant Security Office (CSO) on behalf of the Department of Defense (DoD). As the CSO, DCSA will advise and assist your facility during the FCL process and while you are under our cognizance in the NISP. The requirements, restrictions, and other safeguards that cleared companies must put in place are outlined in the National Industrial Security Program Operating Manual, referred to as the NISPOM. The NISPOM can be located on the DCSA website, at www.DCSA.mil in the Critical Technology Protection section. You are encouraged to review the chapters that are applicable to your security program at this time in order to understand the requirements of the agreement you are about to execute between your company and the US Government (DD Form 441). The NISPOM defines a Facility Clearance as an administrative determination that, from a national security standpoint, a company is eligible for access to classified information at the same or lower classification level as the clearance being granted.

The DCSA Facility Clearance Branch (FCB) recently received a request from a Government Contracting Activity (GCA) or cleared contractor to sponsor your facility for a FCL under the National Industrial Security Program (NISP) for performance on a classified government contract. In order to obtain a Facility Clearance, a company must meet the eligibility requirements listed in the NISPOM 2-102, and meet personnel security clearance requirements for certain essential Key Management Personnel, or KMPs, also discussed in NISPOM chapter 2, section 1. It is important to understand that in order to be eligible for a Facility Clearance, an organization's employees must need access to information that is classified at the Facility Clearance level requested. A requirement to have background investigations to meet position or contract requirements or for access to a physical spaces is *not* the same as a requirement to access classified information and does not meet the eligibility requirement for a Facility Clearance. Please ensure you understand this requirement and how your company meets it, as verification of this will be a point of emphasis throughout the Facility Clearance process.

The below chart represents the first 45 days of the FCL process as well as the follow up after your FCL is issued. Day 1 of this process starts when you receive the Welcome Email identifying specific deadlines for your company and guiding you to register for an account with the National Industrial Security System (NISS).

FCL Roadmap

FCL Orientation Handbook Day 1- Day 5	View FCL Orientation Video Day 5 – Day 10	Complete and submit FCL Package Day 10 – Day 20	FCL Initial Review and e-QIP submission Day 20 - 45	Post FCL Outreach First Year Under NISP
DCSA provides FSOs an educational, user friendly, and informative guide to navigate the FCL process.	FSOs will view the FCL Orientation video on the FCL process (www.dcsa.mil), NISS system, deadlines, and identify documents and forms required per company's business structure	FSOs upload all documents and forms per its company's Business structure into NISS. FCL package is submitted by day 20.	ISRs review company's FCL package and prepare for Initial FCL Orientation meeting. FSOs submit KMP e-QIPs and fingerprints, and prepare for orientation meeting	DCSA reaches out to facilities residing in the NISP under a year, to determine compliance with NISPOM implementation of a facility security program, and assess the facility's potential risk to National Security.

1.0 Overview of the National Industrial Security Program (NISP)

The NISP was established by Executive Order 12829, as amended, 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 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 NISPOM. You will find a link for downloading the NISPOM at the DCSA web site (https://www.dcsa.mil/mc/ctp/nisp/) under the Critical Technology Protection Mission Center. You are expected to review and become familiar with the NISPOM. The FCL Orientation Handbook is not intended to replace the NISPOM. It is simply a guide to inform and assist with navigating the FCL process.

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. DCSA may be able to issue an interim FCL prior to issuance of the final FCL. In order to be issued an interim FCL, DCSA must first validate that there is no unmitigated foreign ownership, control, or influence (FOCI), KMPs have personnel clearances at the interim level or higher, and the initial orientation meeting has been completed.

A final FCL cannot be issued until ALL essential KMP are cleared at the final level of the requested FCL, there are no open changed conditions that would impact the FCL, and the initial orientation meeting has been completed.

If your company has other companies in its legal structure, such as parent or member companies, a decision will be made to either clear or exclude them. The assigned DCSA Industrial Security Representative (ISR) will decide course of action during their review of the documentation in NISS.

Please note: If the essential KMP(s) do not already possess a valid personnel security clearance at the level required for the FCL, your company may experience significant time impacts for issuance of the FCL due to personnel security background investigations and adjudication.

A facility where Foreign Ownership, Control, or Influence (FOCI) is present will also extend time-lines for processing the FCL because these facilities must undergo FOCI analysis and satisfactory FOCI mitigation.

2.0 Facility Security Officer (FSO) Responsibilities and Deadlines

Over the course of the next 45 days it is your responsibility to identify your company's business structure and provide required documentation and forms at the appropriate time. To make this process transparent, the FCL Orientation Handbook provides a roadmap to guide you along the FCL process. In addition to the FCL Orientation Handbook, a FCL Orientation video is available to review as many times as necessary that provides a detailed explanation of the FCL process to include important dates and deadlines. You must first obtain a NISS account prior to submitting any required documentation. Information on NISS can be found at: https://www.DCSA.mil/is/ncaiss/

You can find information to setup your NISS account by accessing the attachment to this handbook titled "Creating an NCAISS Account & Registering for the NISS."

There are three deadlines during the FCL process:

1. Required legal documentation and DCSA forms must be submitted (FCL Package) in NISS within **20 days** of receiving the Welcome E-mail (Day 1)
2. KMP Electronic Questionnaire for Investigations Processing (e-QIPs) must be submitted within **45 days** of receiving the Welcome E-mail (Day 1)
3. KMP fingerprints should be submitted at the same time as the e-QIP submission or **within 14 days** after submitting KMP e-QIPs

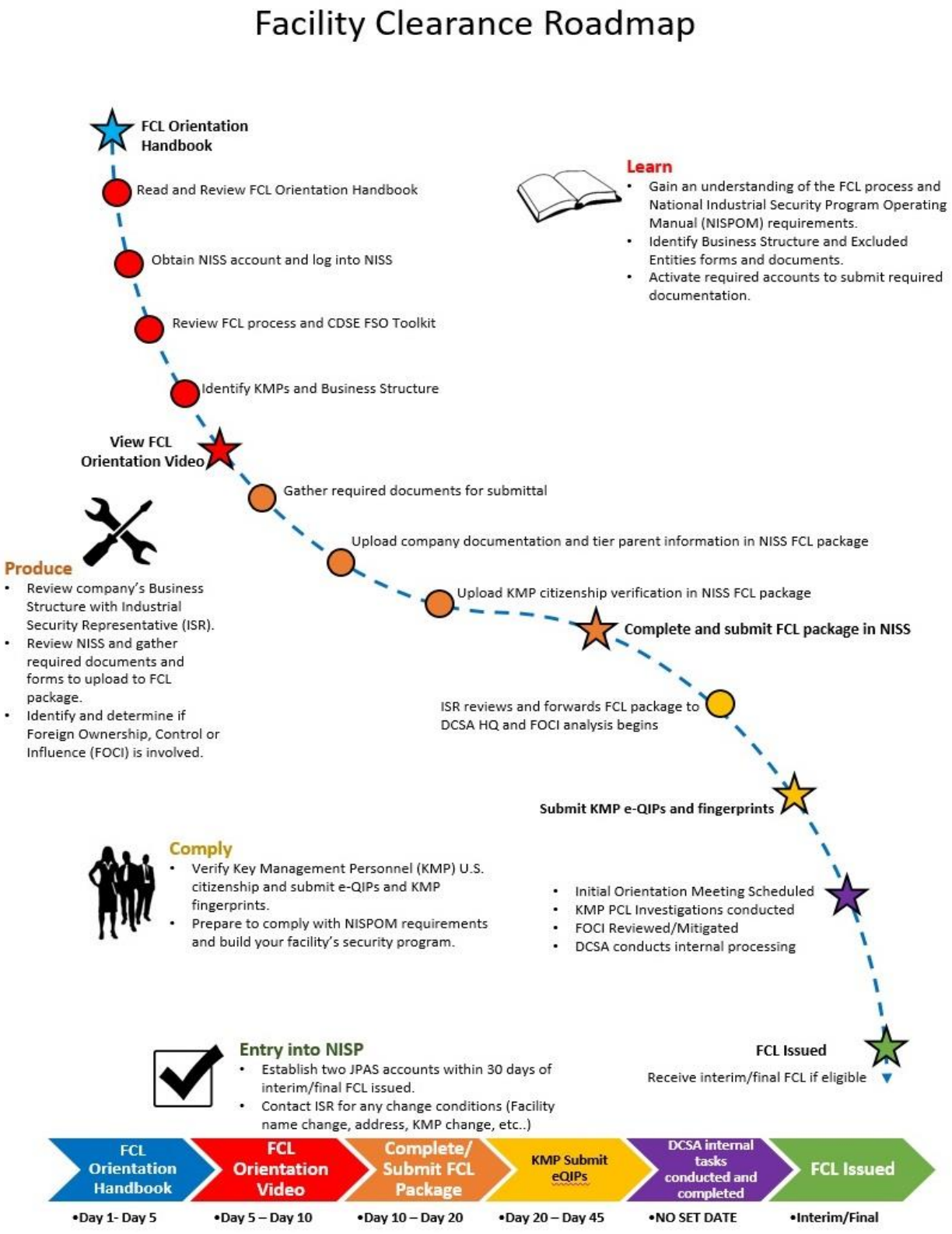
Essential KMP(s) who do not have personnel security clearance eligibility, have not held a personnel security clearance in more than 24 months, or whose background investigations are out of scope will need to complete a Standard Form 86 (SF 86) and submit electronic fingerprints. You will not have access to e-QIP until you receive instructions to do so. An e-QIP will be initiated by FCB, and you will be provided access/submission instructions after your FCL package has been reviewed and approved. It is strongly encouraged that you and all key management personnel obtain a copy of the SF 86 and begin to gather the data that will need to be entered in e-QIP. Please note that the PDF or paper version of the SF 86 cannot be submitted. You must enter this information in e-QIP. However, the questions are the same and the PDF version can be used to assist you in gathering the necessary data.

Electronic fingerprints must be submitted to the Office of Personnel Management, or OPM, via the Secure Web Fingerprint Transmission (SWFT). There are numerous methods for submitting electronic fingerprints. Most companies that are new to the NISP either receive assistance with this from their prime contractor or another cleared company or they use the services of a third party service provider. A list of third party service providers can be found on DMDC's website. Please note that the locations listed are headquarters offices and do not indicate this is the only area the provider serves. Many providers have nationwide locations or provide fingerprint card conversion services, in which a hard copy fingerprint card can be mailed to them for conversion to the proper electronic format and uploaded to SWFT. Whatever method you use, you should verify that the fingerprints are being submitted to OPM via SWFT as many organizations submit fingerprints to other agencies through other systems.

First Year Post FCL Responsibilities:

Once the Facility Clearance Branch (FCB) issues an FCL, you are required to comply with the DoD 5220.22-M "National Industrial Security Program Operation Manual (NISPOM)" and implement a security program. Your company's assigned ISR will reach out 120 days after the FCL is issued to conduct a brief assessment of your facility's compliance with NISPOM requirements and implementation of its facility security program and additionally, per NISPOM Change 2, effective May 2016, an insider threat program.

3.0 FCL Roadmap



4.0 FCL Process Information and Guidance

4.1 FCL Orientation Video

The FCL Orientation Video is a detailed, narrated guide that will walk you through the FCL process. The video is separated into several sections by topic that can be viewed together or separately as often as needed. You are strongly encouraged to take the necessary time to view these videos focusing on specific deadlines that you must meet and required documentation that you must provide in order to move the FCL process forward. Along with the FCL Orientation Handbook, these videos provide all of the information you will need to ensure you have met all requirements for the facility clearance.

If after you have **thoroughly** reviewed the information contained in the video, handbook and attached documents, there are specific, targeted questions, please feel free to contact the DCSA Knowledge Center at 1-888-282-7682, Option #3. Any NISS technical questions should be directed to the NISS Technical Line at Option #2. The Knowledge Center staff will be ready and available to answer those specific, targeted questions; after they have verified that you have viewed the entire video and all sections applicable to your facility.

4.2 FCL Initial Orientation Meeting

The FCL initial orientation meeting is conducted by an ISR assigned from the local field office. Please be prepared to discuss the following topics with the ISR during their on-site visit to the facility:

- Company's NISPOM requirements
- Facility's Security Program
- Facility's Insider Threat Program
- Provide KMP U.S. citizenship verification (current or expired passport or a birth certificate, and government issued photo ID)

4.3 FCL Upgrade Information

If your facility has been sponsored to upgrade the FCL level, the FCL process is largely the same. There are some key differences in the process. The facility should already have an established NISS account, as well as a primary and alternate DISS account holders. The facility still need to submit an FCL package, annotating any changes to the company.

While the FCL package is completed, the KMP list will need to be updated or verified in accordance with any changes the company has made. The KMPs will need to submit new e-QIPs to upgrade their personnel security clearances, if they are not already cleared at the required level for the FCL upgrade. One key difference in the FCL process for an upgrade is the **FSO is responsible for initiating e-QIPs for the KMPs,** and the alternate DISS account holder will initiate the e-QIP for the FSO. The e-QIPs should be initiated once the FSO has submitted the FCL package in NISS. KMPs will be required to submit new

fingerprints, if their personnel security clearance needs to be upgraded due to the change in scope of the investigation.

It is recommended when submitting the NISS FCL package, the FSO update the SF-328 and ensure it is accurate. The facilities FCL package will be reviewed by DCSA HQ once again for analysis of any potential FOCI. If the upgraded FCL is requested within 12 months of the facilities initial FOCI analysis, a new FOCI analysis may not be required. This will be determined by the industrial security representative upon review of the FCL package and in coordination with DCSA HQ.

While all *Initial* FCL packages are reviewed by the Facility Clearance Branch, all FCL upgrades will remain assigned to their local field office, and the FCL packages will be reviewed by the facilities currently assigned industrial security representative. The facility will not be reassigned to the Facility Clearance Branch. The Facility Clearance Branch will continue to oversee and coordinate the FCL process and assist the facility and the industrial security representative.

4.4 FCL Orientation Handbook Attachments

Attached to this handbook (PDF), you will find a number of supplements that are designed to assist you throughout the FCL process. Below is a list of included attachments. Please review these attachments, as they will answer many common questions throughout the FCL process. They will assist in reducing the chances of your FCL package being returned for revision, which may extend the FCL process timelines.

1. Creating an NCAISS Account & Registering for the NISS - Guide
2. DD 441 - Completion Guide
3. External How To Resubmit Initial FCL Package NISS Guide – Guide on how to *RESUBMIT* the FCL package once it has been reviewed and returned for corrections.
4. Guidelines For An Accurate KMP List – Assist in determining KMP to clear or exclude.
5. Initial FCL Process Industry NISS Guide – Will assist in compiling and submitting your initial FCL package.
6. Sample Org Chart – An example of a legal org chart and what should be included/addressed
7. SF328 - Certification Guide – Guide on what signatures are required.
8. SF328 Instructions – Details regarding each question of the SF-328 and what detailed responses are required.

To open the Attachments panel, choose

View > Show/Hide > Navigation Panes >Attachments.

In the Attachments panel, select the attachment.

Double Click the attachment icon to open the attachment in its native application. You may also right click, and save the attachment outside of the FCL orientation handbook.

4.5 FCL Package Submission

Once you have collected and reviewed all your required business documents, it is time to populate the FCL package in NISS. To populate the package and upload documents, you will need to have a NISS account and be using one of the following roles

FSO Role

Alternate FSO Role

Other Security Staff Role

Once the package has been populated with all required information and documents, submit the FCL package for DCSA review. Guidance for submission of the FCL package in NISS can be found in the attachment to this handbook titled "Initial FCL Process Industry." Prior to submitting the FCL package, be sure to review the FCL Package Submission Checklist found in Appendix E. This will assist you in avoiding many common mistakes, which result in the FCL package being returned for revision and may delay the FCL process. After you have submitted the FCL package, ensure the FCL Package status has been updated to "Submitted." This will ensure that any potential NISS workflow issues are quickly identified and remedied.

5.0 Business Structure and Excluded Tier Entities

The following section details the required business structure and excluded tier entity forms and documents to submit in your company's FCL Package in NISS.

Please note: In accordance with ISL 2006-02, #12 when only one person within an organization requires access to classified information and that person and members of their immediate family are the sole owners of the organization, that person should work as a consultant and would not require a Facility Clearance.

5.1 Business Structure Required Documents

Business Structure	Business Records Required	PCLs for KMPs
Sole Proprietorship	▪ Business License ▪ Fictitious Name Certificate ▪ Recent changes to company Structure	▪ Owner of sole proprietorship ▪ Senior Management Official (SMO) ▪ FSO ▪ ITPSO
General Partnership	▪ Business License ▪ Fictitious Name Certificate ▪ Partnership Agreement ▪ Legal Organization Chart ▪ Board/Company Meeting Minutes ▪ Recent changes to company Structure ▪ FSO/ITPSO Appointment Letter ▪ KMP Citizenship Verification ▪ Signed undated DD Form 441 ▪ Signed SF 328	▪ SMO ▪ FSO ▪ ITPSO ▪ All General Partners, *except*: Single Partner (must be cleared) Management Committee (all committee members must be cleared)
Limited Partnership	▪ Business License ▪ Fictitious Name Certificate ▪ Partnership Agreement ▪ Certificate of Limited Partnership ▪ Legal Organization Chart ▪ Board/Company Meeting Minutes ▪ Recent changes to company structure ▪ FSO/ITPSO Appointment Letter ▪ KMP Citizenship Verification Signed undated DD Form 441 ▪ Signed SF 328	▪ SMO ▪ FSO ▪ ITPSO ▪ All General Partners, *except*: Single Partner (must be cleared) Management Committee (all committee members must be cleared) ▪ Limited Partners need PCL if they work on classified contracts or need access to classified information
Joint Venture (JV)	▪ Business License ▪ Fictitious Name Certificate ▪ JV Agreement ▪ Legal Organization Chart ▪ Board/Company Meeting Minutes ▪ Recent changes to company Structure ▪ FSO/ITPSO Appointment Letter ▪ KMP Citizenship Verification Signed undated DD Form 441 ▪ Signed SF 328	▪ SMO ▪ FSO ▪ ITPSO ▪ JV Partners must be excluded or cleared if their duties require access to classified information ▪ Officials working on JV are cleared if their duties require access to classified information

Business Structure	Business Records Required	PCLs for KMPs
Privately Held Corporation	▪ Business License ▪ Fictitious Name Certificate ▪ Articles of Incorporation ▪ By-Laws ▪ Stock Ledger ▪ Legal Organization Chart ▪ Board/Company Meeting Minutes ▪ Recent changes to company ▪ structure ▪ FSO/ITPSO Appointment Letter ▪ KMP Citizenship Verification ▪ Signed undated DD Form 441 ▪ Signed SF 328	▪ SMO ▪ FSO ▪ ITPSO ▪ Chairman of the Board ▪ Vice Chair of Board, if provisions for rotating or Pro Tem duties ▪ Corporate Officials are cleared if their duties require access to classified information
Publicly Held Corporation	▪ Business License ▪ Fictitious Name Certificate ▪ Articles of Incorporation ▪ By-Laws ▪ Stock Ledger ▪ Most recent SEC filings ▪ Legal Organization Chart ▪ Board/Company Meeting Minutes ▪ Recent changes to company Structure ▪ FSO/ITPSO Appointment Letter ▪ KMP Citizenship Verification ▪ Signed undated DD Form 441 ▪ Signed SF 328	▪ SMO ▪ FSO ▪ ITPSO ▪ Chairman of the Board ▪ Vice Chair of Board, if provisions for rotating or Pro Tem duties Corporate Officials are cleared if their duties require access to classified information classified information
Limited Liability Company	▪ Business License ▪ Fictitious Name Certificate ▪ Certificate of Formation or Articles of Organization ▪ Legal Organization Chart ▪ Operating Agreement ▪ LLC Meeting Minutes ▪ Recent changes to company ▪ structure ▪ FSO/ITPSO Appointment Letter ▪ KMP Citizenship Verification ▪ Signed undated DD Form 441 ▪ Signed SF 328	▪ SMO ▪ FSO ▪ ITPSO ▪ LLC Members are cleared if their duties require access to classified information ▪ Managers
College/University	▪ Charter ▪ Board/University Meeting Minutes ▪ Legal Organization Chart ▪ Recent changes to university Structure ▪ FSO/ITPSO Appointment Letter ▪ KMP Citizenship Verification ▪ Signed undated DD Form 441 ▪ Signed SF 328	▪ SMO ▪ FSO ▪ ITPSO ▪ President ▪ Regents/Trustees/Directors are cleared if their duties require access to classified information

*****Include the most recent Meeting Minutes and any Meeting Minutes to reflect changes to a company's address, name, KMPs, etc. which may be different than the operating agreement/by-laws etc.
****** If Business Structure is not identified, discuss with your ISR or contact the DCSA Knowledge Center at 1-888-282-7682, Option #3

Legal Organization Chart (see Appendix D) must be submitted in the FCL Package. It shall reflect all U.S. and foreign parent companies and subsidiaries including their affiliates. The Legal Organization Chart shall identify the associations between the cleared facilities and the ultimate parents, including the

percentages of ownership, FCL status, CAGE codes and other helpful information explaining the relationship among the companies in the chain of ownership.

Excluded KMPs: DCSA will determine which Officers and Directors of the company not accessing classified information are considered excluded, and do not need a PCL. The company must submit exclusion resolutions for these Officers and Directors (see Appendix B).

If Key Management Personnel are cleared for contractual performance reasons and not in connection with the FCL then this difference needs to be identified.

**FOR MORE INFORMATION ON KMP ROLES SEE APPENDIX A

5.2 Required Forms

Forms	To Include on Forms
SF 328; Certificate Pertaining to Foreign Interests	▪ Certificate pertaining to a company's foreign interests ▪ Execute two original SF 328 forms for DCSA and contractor retention ▪ SF 328 must be signed by an employee or representative of the company who has actual authority to execute agreements with the U.S. Government on behalf of the company, such as the SMO ▪ One witness signature is required ▪ Upload signed SF 328 into NISS ▪ Provide all supplemental responses to affirmative SF 328 questions ▪ SF 328
Key Management Personnel (KMP) Form - NISS	▪ Spell out entire KMP names ▪ Social Security Number not required for excluded KMPs ▪ KMPs **must** match the Articles of Organization, by-laws or amendments
Proof of Citizenship If applicable	▪ Citizenship verification in the form of a U.S. Passport, Birth Certificate, or Certificate of Naturalization for all KMP(s) requiring personnel security clearance processing.
DD Form 441	▪ Agreement between your organization and the United States Government that details the security responsibilities of both the cleared organization and the United States Government ▪ Execute two original DD 441 forms for DCSA and contractor retention. ▪ DD 441 must be signed by an employee or representative of the company who has actual authority to execute agreements with the U.S. Government on behalf of the company, such as the SMO. ▪ One witness signature is **required** ▪ Upload signed DD 441 into NISS ▪ **The date on page 1 and the Government Representative section on page 2 should be left blank.** ▪ DD Form 441
DD Form 441-1 If applicable (Cleared branches/divisions)	▪ Attachment to the DD Form 441 listing cleared divisions or branch offices that are included in and covered by the provisions of the organization's Security Agreement and Certificate Pertaining to Foreign Interest. ▪ DD Form 441-1

- As a general note for all business types, organizations must register their business with a physical address. The physical address is the actual address where the organization is located and does not have to be in the state of incorporation/organization. This is the address DCSA uses for the Facility Clearance and is considered the home office. The CAGE code registration must also match this address. Organization may also have a registered agent address, which typically must be in the state of incorporation/organization and is usually the address documents and notices, such as annual report filings, are mailed to by the Secretary of State.

- Some states and jurisdiction do not require certain types of organizations to have all documents referenced. In these cases, it may be very difficult for DCSA to determine if and when the organization meets NISPOM requirements. Some documentation outlining the governance and structure of the organization and the roles and responsibilities of the organization's officials **will be required** to determine eligibility for a Facility Clearance.

6.0 Specific Business Structure Guidance

6.1 Corporation:

The business documents required for a privately or publicly held corporation include the Certificate or Articles of Incorporation, which are filed with the Secretary of State's office in the state or jurisdiction where the corporation is incorporated, Corporate Bylaws describing the rules governing the regulation of a corporation's internal affairs, initial and most recent Shareholder and Board of Directors Meeting Minutes, as well as those approving any significant changes to the Corporation, a stock ledger listing the individuals and organizations that hold stock in or shares of the corporation or SEC filings for publicly-held corporations, and a legal organization chart showing the corporation's ownership and its connections to other business entities. You may also wish to include a legal organization chart showing the internal management structure of the company.

The KMP list for a corporation must include all directors, and officers.

Shares or stock of a corporation may be held by either people or other organizations. If held by people, these people are called share or stock holders and may be listed on the KMP list with their ownership percentages. If organizations hold stock, they are considered "tiered parents" and should be listed in "Package Summary Comments for DCSA" under the "Industry-DCSA Package Comments" section of the FCL package in NISS. Shareholder control and authority varies. Shareholders, either people or organizations, are not typically required to be cleared simply because they are shareholders. However, if they have significant control or authority over the cleared corporation, they may require a clearance.

Directors, not including the Chairman of the Board, typically do not hold authority that would prevent them from being effectively excluded but this may vary from corporation to corporation. The Chairman of the Board must **always** be cleared. If a corporation has a rotating Chairman, those who may hold this position must be cleared to the appropriate level prior to filling the role and should be processed for clearances accordingly.

In most corporations, those holding the titles of Chief Executive Officer and President typically hold the highest day-to-day management authority, and must be cleared. Most corporations also have a Secretary and Treasurer and possibly a Vice President or Vice Presidents. Traditional authority associated with these roles would allow them to be effectively excluded. Other officer titles designated in the bylaws must also be listed on the KMP list. Typically, these officers report to the CEO or President and can be effectively excluded.

For all shareholders, directors, and officers, each corporation should review the authorities and roles and compare these to the exclusion criteria in NISPOM 2-106 and the typical responsibilities associated with each role described in the Facility Clearance Orientation Handbook to make a preliminary determination about whether or not they can be effectively excluded. The assigned Industrial Security Representative will make the final decision regarding exclusion upon analysis of the corporation as a whole.

Finally, the FSO and ITPSO must be listed on the KMP list and must be cleared or processed for a personnel security clearance at the level of the facility clearance requested.

6.2 LLC:

The business documents required for a Limited Liability Company, or LLC, include the Certificate or Articles of Organization, which are filed with the Secretary of State's office in the state or jurisdiction where the company is organized, an Operating Agreement, which describes the governance of the LLC's business and financial and managerial rights and duties, initial and most recent Member or Manager Meeting Minutes, as well as those approving any significant changes to the Company, a membership ledger that lists the individuals and organizations that hold membership interest in the company, and a legal organization chart showing the company's ownership and its connections to other business entities. You may also wish to include a legal organization chart showing the internal management structure of the company.

The KMP list for an LLC must include all members, if people, and managers, as well as officers, if they are described in the company's Operating Agreement.

LLCs are a relatively new business structure that allows for greater flexibility than the traditional business structures. As a result, their setup can vary widely. The legal requirements for an LLC also vary widely by state and jurisdiction.

Members of an LLC are the owners of the company, similar to shareholders of a corporation, and may be people or other organizations. In an LLC, the management of the company is either automatically vested in the members by virtue of their being members (called "member-managed") or vested in a separately designated manager, managers, or board of managers (manager-managed). Members are not generally required to be cleared simply because of their ownership interest. However, this will vary depending on their specific authority to control or influence the business as described in the LLCs operating agreement.

Managers of an LLC are generally required to be cleared as it is extremely rare that they have a level of authority that would allow them to be effectively excluded. In an LLC with multiple managers with varying levels of interest or a Board of Managers or similar executive body, this may vary. However, the chairman or manager with majority interest will almost definitely be required to be cleared.
Due to the flexibility of an LLC, LLCs may create corporate-style officer positions but this is relatively rare. Often, members and managers refer to themselves using corporate-style titles, such as CEO and President, because they are more recognizable in the business world, without outlining these in the business documents. For the purpose of the KMP list for DCSA, companies should enter **any and all** titles that are outlined in business documents and refrain from including titles that are only used in practice. Whether or not the individuals in these positions require a clearance will depend on their role as described in the business documents. These titles vary from being essentially "in name only" titles to holding responsibility similar to that of a corporation so they can be difficult to assess.

Please note that because of the flexibility of LLCs, it is possible to have an LLC that is owned by another organization and member-managed, making the owning organization the manager. Most organizations that are set up this way did this by default without fully explaining how the owning organization would "manage" the day-to-day operations of the LLC. In most cases, the way these LLCs are operating does not align with the description in their business documents. It can be extremely difficult for DCSA to determine if and when these LLCs meet NISPOM requirements for a facility clearance.

The FSO and ITPSO must be listed on the KMP list and must be cleared or processed for a personnel security clearance at the level of the facility clearance requested.

6.3 Partnership:

There are three common types of partnership: General Partnerships, Limited Partnerships, and Limited Liability Partnerships although other types may exist in some states or jurisdictions. A General Partnership consists of all General Partners. A Limited Partnership consists of one or more General Partners and one or more Limited Partners.

Limited Liability Partnerships are more similar to LLCs, with Partners being similar to Members, and are formed through Articles of Organization. For the purpose of this section, we will focus on General Partnerships and Limited Partnerships

For Limited Partnerships, a Certificate of Limited Partnership is filed with the Secretary of State's office. General Partnerships are typically formed without official registration with a Secretary of State, although some jurisdictions may require a Business License, a Fictitious/Trade Name Registration, or other similar documentation. Regardless, General Partnerships must provide documentation to DCSA that demonstrates their legal existence as a General Partnership, the name they are doing business under, and the jurisdiction whose laws they are organized and operating under.

Note that organizations that use General Partnership, General Partners, or GP in the name are rarely actually General Partnerships. Most often, they register as another business type such as an LLC. For example, ABC General Partners, LLC is an LLC and not a General Partnership for the purpose of NISP participation and you should refer to the section of this Orientation on LLCs for the business document and KMP requirements. However, if there is a Partnership Agreement in addition to an Operating Agreement in this scenario, both should be provided to DCSA.

A partnership agreement is a contract between two or more business partners that establishes the responsibilities of each partner and general rules about the partnership. Partnership Agreements may not be required for all partnership types in all states. However, DCSA will need to be provided with some documentation that outlines the responsibilities of the partners and the basic rules and structure of the partnership in order to determine if or when it meets the eligibility requirements for a Facility Clearance. You must provide a legal organization chart showing the partnership's ownership and any connections to other business entities. You may also wish to include a legal organization chart showing the internal management structure of the company.

The KMP list for a General or Limited Partnership should include all General and Limited Partners who are people. General or limited partners that are organizations must alternatively be listed in "Package Summary Comments for DCSA" under the "Industry-DCSA Package Comments" section of the FCL package in NISS.

General partner is the name given to partners that have active involvement in managing the partnership. As such, General Partners must be cleared. Both General Partnerships and Limited Partnerships have at least one General Partner.

Limited partner is the name given to a partner that does not participate in management of the business. As such, Limited Partners can generally be effectively excluded. General Partnerships do not have any Limited Partners. Limited Partnerships may have one or more Limited Partners in addition to their General Partner(s). Like Members of an LLC and Shareholders of a Corporation, Partners may be people or other organizations. If a General Partner is an organization, it must be clear in business documents

what person or people are managing the business and how they are doing so. If this is not clear in business documents, it may be difficult or impossible for DCSA to determine when or if the Partnership meets eligibility requirements for a Facility Clearance.

The FSO and ITPSO must be listed on the KMP list and must be cleared or processed for a personnel security clearance at the level of the facility clearance requested.

6.4 Educational Institute:

Educational institutions vary widely in how they are established and governed, which may change the required business documents and KMP identification significantly. Each institution should review its record thoroughly and compare its structure to that of other business types, if applicable.
In general, a charter is given by provincial, state, regional, and sometimes national governments to legitimize the university's existence. If the charter does not describe how the organization is run and who has authority to manage the organization, a separate document, such as bylaws or a constitution, must be provided.

Board Meeting Minutes from a Board of Regents/Trustees/Directors/Managers or other executive or governing board must be provided if they are needed to support existence of or significant changes to the organization or the designation or elections of members of the board or officers.

A legal organization chart must be provided to show the organization's ownership, if applicable, and any connections to other business entities. You may also wish to include a legal organization chart showing the internal management structure of the organization.

The KMP list for colleges and universities varies. However, in general, it must include all officials described as having a role in the governance of the organization in governance documents.

Typically, the President of a University or College is the highest management authority and must be cleared. The management of the business affairs of the organization may be accomplished through a Board of Regents/Trustees/Directors/Managers or other type of executive or governing body. Depending on their level of authority, all or some may be able to be effectively excluded. However, a chairman or quorum may need to be cleared. In a college or university, another official, such as a program manager or director, may be responsible for classified contracts. This person must be cleared.

The FSO and ITPSO must be listed on the KMP list and must be cleared or processed for a personnel security clearance at the level of the facility clearance requested.

6.5 Sole Proprietorship:

The requirements for legal registration of a sole proprietorship vary by state and jurisdiction and there are often multiple options. DCSA requires documentation demonstrating that the sole proprietorship is legally organized and existing as a sole proprietorship and identifying the jurisdiction whose laws it is operating under. Depending on the state, this may be a business license, a fictitious name certificate, a certificate of sole proprietorship or another similar document.

The KMP list for a sole proprietorship must include the sole proprietor. The sole proprietor is the owner

of a sole proprietorship and must always be cleared to the level of the Facility Clearance.

Additionally, the FSO and ITPSO must be listed on the KMP list and must be cleared or processed for a personnel security clearance at the level of the facility clearance requested.

6.6 Branch or Division Office:

A branch office or division is a separate location of an existing legal entity, referred to as a multiple facility organization (MFO). Because a branch office is part of the same legal entity as its home office, they must have the same legal name. In most cases, only the home office requires a facility clearance. A branch office or division only requires a separate Facility Clearance issued by DCSA if it will need to be able to safeguard collateral classified information within that office. If it will need to exclusively safeguard classified information that is not under DCSA cognizance, a Facility Clearance issued by DCSA is not required, but other requirements will need to be met as determined by the organization that does have cognizance. If no safeguarding is needed at the branch office, administrative security requirements, such as personnel security clearance processing and training, are handled by the home office via its security program.

For branch offices that do require a Facility Clearance, the home office must always be cleared to the same or a higher level as the branch office. If you are a branch office or division and your home office is not cleared or in-process for a facility clearance, please contact the DCSA Knowledge Center immediately. Because the majority of the legal business documents and forms required are provided by the home office, the FCL package requirements for a branch office or division are minimal. The required documents include any business records of the legal entity that apply specifically to the branch office, such as meeting minutes establishing a new office location, a KMP list, a DD Form 441-1, which is signed by home office, and a legal organization chart.

The KMP list for a branch office is the only type of KMP list in which the individuals listed are not required to be designated in legal business documents. The KMP list for a branch office should include a SMO specific to the site, which is the person who has senior management authority at that office, the branch office FSO and the ITPSO. The ITPSO must be listed on the branch office KMP list even if this is a corporate-wide ITPSO.

6.7 Joint Venture:

Joint Ventures are becoming more and more popular. Joint Ventures, or JVs, can be formed in a couple of ways.

A JV by Contract is generally a team of two or more legal business entities that has entered into a contract together to work on a specific project. They do not form a separate legal operating entity, but have a contract that outlines the terms of their arrangement.

Alternatively, a JV can be formed following a similar agreement between two or more organizations to form a legal operating entity, such as a Corporation, an LLC, or a Partnership to serve as the JV.

There are 2 key points to consider with JVs:

First, in accordance with NISPOM 2-102b, in order to be eligible for a Facility Clearance, an organization must be legally organized and existing in the United States. Therefore, JVs by contract that have not formed a legal registered operating entity are not eligible for a Facility Clearance.

Second, JVs may be either populated or unpopulated. This means that the JV entity either itself has employees or does not have employees, in which case the employees remain employees of the organizations that make up the JV. In accordance with NISPOM 1-201, 1-202b, 2-104, the FSO, the ITPSO, and the SMO must be employees of the organization holding the Facility Clearance. Therefore, the JV must have an employee(s) who hold these positions. There may be regulations that provide that a JV may not be populated with individuals intended to perform on contracts awarded to the JV (13 CFR 121.103 (h)). That is, the JV may have its own separate employees to perform administrative functions, but may not have its own separate employees to perform on contracts awarded to the JV. Note that this scenario does not conflict with the NISPOM requirements to have employees performing administrative security functions.

If a classified contract is awarded to the JV, the JV needs a Facility Clearance. If the contracts is exclusively awarded to one or both JV partners, those organizations require Facility Clearances.

Business records and KMP requirements are determined by the type of legal entity. For example, many JVs organize as LLCs. This organization should have Articles of Organization, and an Operating Agreement. Although, it may also have a JV Agreement or it may cover the operation of the organization as both an LLC and a JV in one or the other. Both the Operating agreement and the JV Agreement should be provided to DCSA, if both exist.

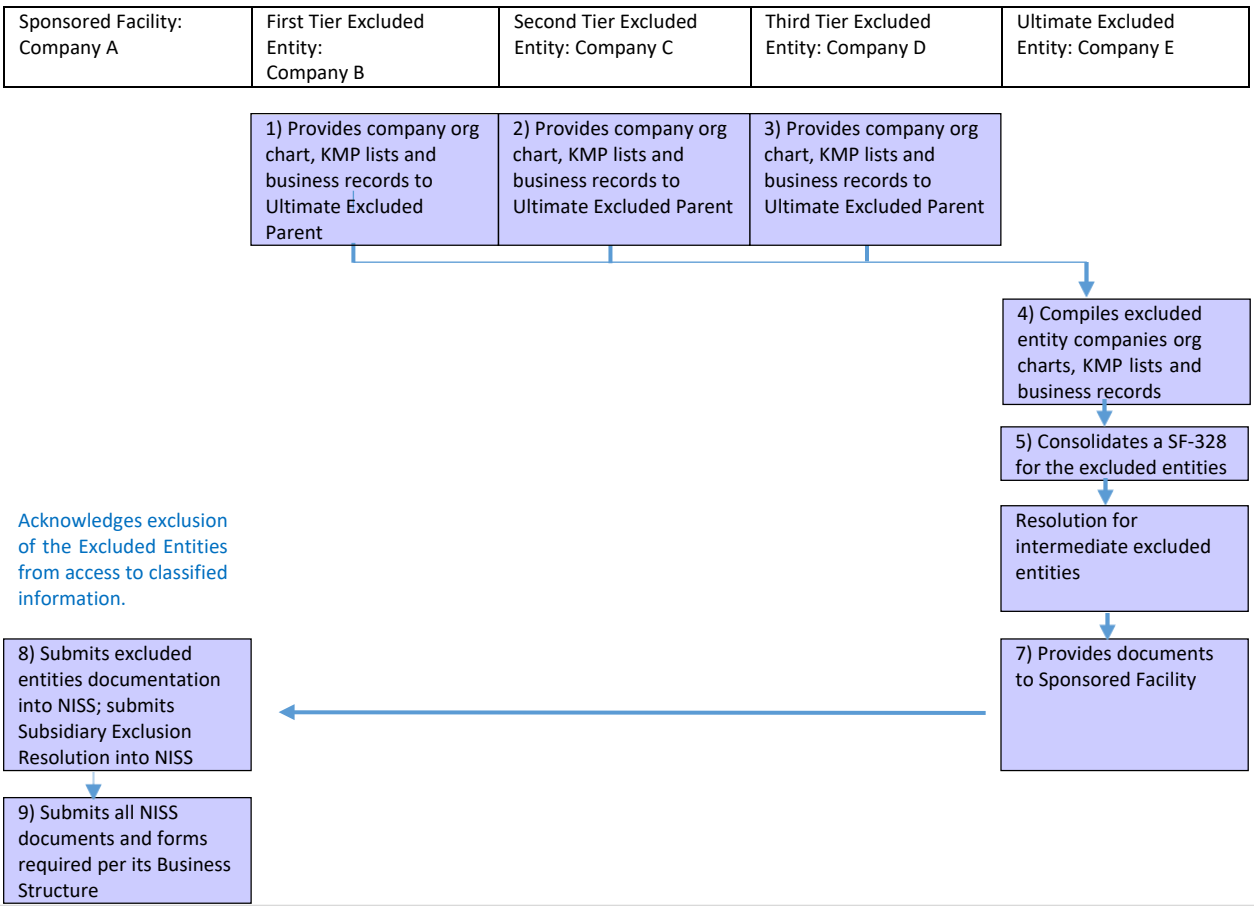
7.0 Excluded Tier Entity Process

The objective of this process is to clear the sponsored facility and identify tiered companies to exclude from access to classified information. A tiered company, also known as a parent company, is defined as a company owning at least a majority of another company's voting securities. DCSA determines if tiered companies are required to obtain an FCL or can be excluded from access to classified information. If a tiered company needs to be cleared, it will also be placed in process and cleared concurrently with the company that was awarded the contract. This will be determined by the industrial security representative.

NOTE: Parent companies should be identified in "Package Summary Comments for DCSA" under the "Industry-DCSA Package Comments" section of the FCL package in NISS. Please include the parent company's legal name, CAGE Code, address, and a designated Point of Contact's name, email address and phone number.

7.1 Excluded Tier Entity Requirements

The process flow below outlines the required documents the sponsored facility must provide to DCSA on behalf of any intermediate excluded entities and the ultimate excluded entity. In this process neither the ultimate excluded entity nor any of the intermediate tiered entities hold a FCL.



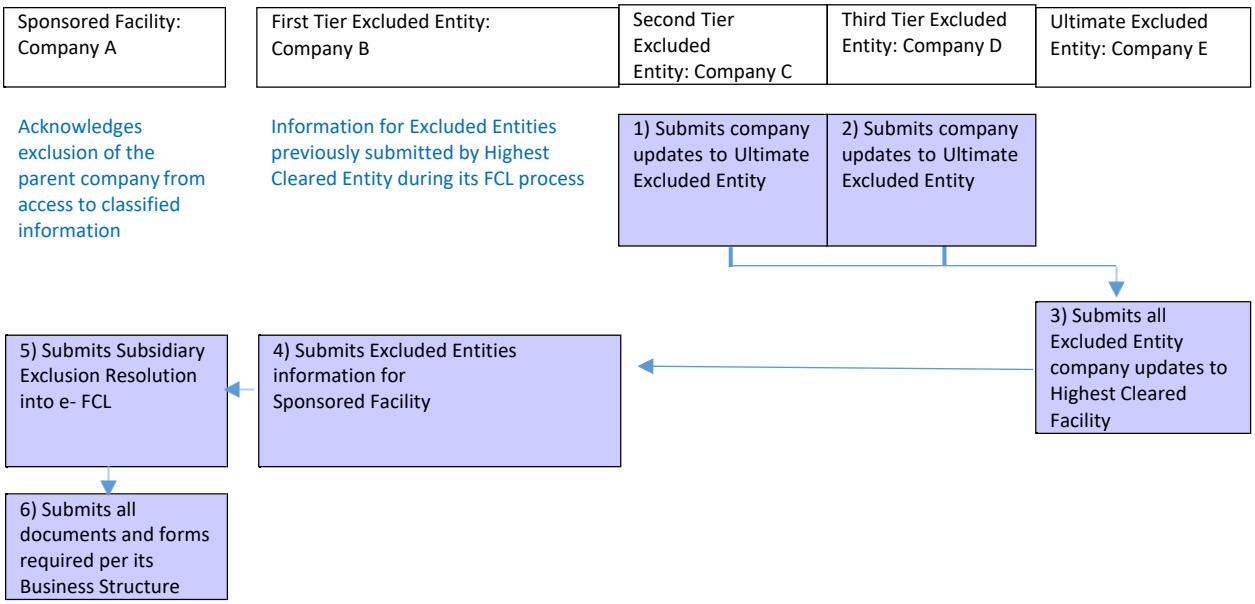
7.2 Entity Roles and Responsibilities

Entity	Responsibility
Intermediate Parent/Owner Entity	▪ Submits Company's Organization Chart, KMP List, and Business Records to Ultimate Cleared Entity
Ultimate Parent/Owner Entity	▪ Provides all Entities Organization Charts, KMP Lists, and Business Records to Sponsored Facility ▪ Provides Sponsored Facility the requested Exclusion Resolution on behalf of its company and Intermediate parents to be Excluded
Sponsored Facility (Highest Cleared Facility)	▪ Submits Parent entities to be Excluded Organization Charts, KMP Lists, Business Records, and Exclusion Resolution for entities ▪ Submits Subsidiary Exclusion Resolution acknowledgement ▪ Submits all required NISS Forms and Documents per its Business Structure

8.0 Highest Cleared Tier Entity

The process flow below documents the required documents the Sponsored Facility and Highest Cleared Entity must provide to DCSA on behalf of any Intermediate Excluded Entities and the Ultimate Excluded Entity. In this process the Highest Cleared Entity holds a FCL and provides DCSA updates on behalf of the Ultimate Excluded Entity and Intermediate Tier Entities. Highest Cleared Entity previously submitted all required Documents and Forms for Excluded Entities during its FCL process.

8.1 Process Flow



8.2 Entity Roles and Responsibilities

Entity	Responsibility
Intermediate Entity	▪ Submit changes to Ultimate Entity, if applicable
Ultimate Entity	▪ Provides Intermediate Entity changes to Highest Cleared Entity, if applicable
Highest Cleared Entity	▪ Provides Entity changes to DCSA, if applicable
Sponsored Facility	▪ Submits all required NISS Forms and Documents per its Business Structure ▪ Submits Subsidiary Acknowledgement of Exclusion Resolution

9.0 Accounts and Systems

The table below outlines the Accounts and Systems the FSO must activate or leverage to submit additional documents for its Facility to receive its FCL and to maintain a compliant security program after obtaining the FCL.

Accounts	Reason for Account	Description
Commercial and Government Entity (CAGE) Code	Provides a standardized method to identify your Specific facility	The CAGE Code is a five-character ID number used extensively within the federal government, assigned by the Department of Defense's Defense Logistics Agency (DLA). If your company does not already have a CAGE Code for the facility requiring clearance, one may be obtained by visiting System for Award Management (SAM) or DLA CAGE if you are a subcontractor. **SAM LINK**
Joint Personnel Adjudication System (JPAS)	System to serve as the record to perform comprehensive personnel security, suitability, and credential eligibility management. *****_Account MUST be established within 30 days of the FCL being issued._	JPAS is the system of record (until April 2021 when DISS fully deploys) for personnel security clearances. All PCL eligibility and access records for KMPs and those requiring access to classified information must be kept up-to-date in JPAS. Because a person cannot view or take action on their own JPAS record, **cleared companies must have at least two (2) JPAS account holders** to comply with NISPOM requirements. The Defense Manpower Data Center (DMDC) is the functional manager of JPAS. Full JPAS Account Request procedures are available on their website. **JPAS LINK**
Defense Information System for Security (DISS)	System to serve as the record to perform comprehensive personnel security, suitability, and credential eligibility management.	Once fully deployed (APR 2021), DISS will replace JPAS. DISS provides secure communications between Adjudicators, Security Officers, and Component Adjudicators in support of eligibility and access management. All PCL eligibility and access records for KMPs and those requiring access to classified information must be kept up-to-date in DISS. Because a person cannot view or take action on their own DISS record, **cleared companies must have at least two (2) DISS account holders** to comply with NISPOM requirements. The Defense Manpower Data Center (DMDC) is the functional manager of DISS. Full DISS Account Request procedures are available on their website. **DISS LINK**
Electronic Questionnaires for Investigations Processing(e-QIP)	Submit KMP information through this system as part of the PCL process	e-QIP allows the user to electronically enter, update and transmit their personal investigative data over a secure internet connection to a requesting agency. **E-QIP LINK**
National Industrial Security System (NISS)	System of Record for Facility Clearances *****_NISS is behind a system called the NISP Central Access Information Security System (NCAISS). This web-based application provides PKI-based authentication for DCSA applications. You will need a PKI certificate to obtain access to NCAISS and NISS._	NISS replaces and expands upon capabilities of two legacy systems, ISFD, and e-FCL, and automates the Initial Facility Clearance process. This system also expands access and transparency to security professionals' facility information. **NISS LINK**
Secure Web Fingerprint Transmission (SWFT)	Submit KMP fingerprints through SWFT or third party vendor to complete KMP's PCL process *****_Account created after Facility is issued its FCL._	SWFT allows the submission of fingerprints to be uploaded electronically through its system. (All fingerprint images that are provided in support of background investigations must be captured and submitted electronically) _For SWFT access, submit DMDC's new Personnel Security System Access Request (PSSAR) form to the DMDC Contact Center for processing_ **SWFT LINK**
Security Training, Education, and Professionalization Portal (STEPP)	Provides courses for Contractor's security professionals	Program maintaining the list of courses DCSA provides to security professionals. The courses are intended for use by Department of Defense and other U.S. Government personnel and contractors within the NISP. **STEPP LINK**

National Industrial Security Program (NISP) Enterprise Mission Assurance Support Service (eMASS) *(See Appendix C for details.)*	Provides standardized Risk Management Framework (RMF) process support and storage for cyber security artifacts for assessment by cleared industry and DCSA security professionals *****Account Requirements:* - Complete DISA eMASS Training - Complete DoD Cyber Awareness Challenge - Submit DD 2875 SAAR	eMASS is an application that automates the DCSA Assessment and Authorization Process Manual (DAAPM) tasks supporting the Risk Management Framework (RMF) used by the Department of Defense, other US Government Agencies, and the NISP industry participants. The NISP eMASS instance is available at the link. **NISP eMASS Link**

10.0 Training

Training Classes	Link
Center for Development of Security Excellence (CDSE) Toolkits	https://www.cdse.edu/toolkits/index.html
FSO Toolkit	https://www.cdse.edu/toolkits/fsos/index.php
ITPSO Toolkit	https://www.cdse.edu/toolkits/insider/index.php
DCSA Risk Management Framework Toolkit **RMF Knowledge Service** (*See Appendix C for details.*)	https://www.dcsa.mil/mc/ctp/tools/ https://rmfks.osd.mil/rmf/Pages/default.aspx

The CDSE Toolkits are a repository of role-based resources that serve as a one-stop shop for security essentials. Each toolkit points you to the resources you need to help perform your role. The FSO Toolkit and Insider Threat Toolkit will be one of your most important resources while you are participating in the NISP.

10.1 FSO Training

A list of the required FSO Training is available in the FSO Toolkit. FSO's of companies that will require safeguarding should sign up for the FSO Program Management for Possessing Facilities. FSO's of companies that do not require safeguarding should sign up for FSO Orientation for Non-Possessing Facilities. Both courses are offered on the Security Training, Education and Professionalization Portal, or STEPP, which is available on the DCSA website under Information Systems. You will need to take each course as well as the corresponding exam. The sooner you take this training, the easier it will be to set up your security program and understand your requirements under the NISP.

10.2 Insider Threat Program Training

The requirements for your Insider Threat Program can be found in NISPOM 1-202 and ISL 2016-02. You are required to nominate an Insider Threat Program Senior Official (ITPSO). This person will be considered a KMP along with the FSO, SMO, and other KMP(s). The ITPSO can be the same individual as the FSO, or it can be a different person. Corporate families are able to nominate a corporate ITPSO.

The ITPSO MUST take the training listed below within 30 days of being formally appointed ITPSO. The ITPSO may choose to use an existing training course to meet this requirement called Establishing an Insider Threat Program for your Organization. This course is offered on STEPP, which is available on the DCSA website under Information Systems.

- Establishing an Insider Threat Program for Your Organization INT122.16
- Insider Threat Awareness Course INT101.16

The ITPSO must also certify that a written Insider Threat Program is in place. Your ISR will talk to you more about this when they are onsite for the Initial Orientation Meeting. Additional information, including a plan template and job aid, is available at the Industry Insider Threat and Resources link in the most requested links section of the DCSA website.

Appendix A: Defining KMP Authorities of Position

KMP Role	Authorities of the Position
CEO	▪ Highest ranking executive manager in a corporation or organization's by-laws or organizational documents ▪ Responsible for the overall success/management of the organization ▪ Ultimate authority to make final decisions for an organization ▪ Responsibility for creating, planning, implementing, and integrating the strategic direction/vision of an organization ▪ Reports to a Board of Directors and serves at the discretion of the ▪ Board of Directors
President	▪ Creates, communicates, and implements the organization's vision, mission, and overall direction ▪ Leads, guides, directs, and evaluates the work of other executive leaders including senior vice presidents, vice presidents and directors ▪ Formulates and implements the strategic plan that guides the direction of the business ▪ Oversees the organization in accordance with the direction established in the strategic plans
Chairman of the Board	▪ Trusted with the responsibility of chairing a board or organization ▪ Governs the board according to the bylaws of the organization. The chairman must attend the board meetings and committees regularly. ▪ Committed to board duties and has vast knowledge of the organization itself ▪ Evaluates annual performance of the organization ▪ Chairman rarely involves themselves in the company's day-to-day operations, instead concentrating on the bigger picture and various strategies to increase the company's bottom line ▪ Institutes company policies and guidelines, and make certain that they are carried out via upper management ▪ Recruits, interviews, and hires the CEO ▪ Votes on key issues surrounding the company; when board is at a standstill on an issue, the chair makes the final decision
Manager	▪ For an LLC, only a manager or authorized officer can bind the LLC as specified in the Operating Agreement or when there is no operating agreement, State Law where LLC is formed ▪ Elected by the members ▪ Decision authority on key policies, transactions, and establishment of guidelines for how the LLC will operate ▪ Can appoint officers to serve at the pleasure of the manager
General Partner	▪ Full management control and also accepts full personal responsibility for partnership liabilities as specified by state law where the partnership was formed and the partnership agreement ▪ Right to manage the business, conduct transactions on the behalf of the business, and are liable for the business' debts ▪ Commonly is active in the day-to-day operations of the business ▪ May be an individual or company
Shareholder	▪ Makes a financial investment in the corporation, which entitles those with voting shares to elect the directors as specified in the Shareholders agreement and/or state law ▪ Does not normally have any rights to be involved directly in company management ▪ Connection to company management is typically via the Board of Directors ▪ If shareholder is not satisfied with the performance of the directors, ▪ they may remove the directors or refuse to re-elect them

KMP Role	Authorities of the Position
Board of Director	▪ Protects shareholders' assets and ensure they receive a decent return on investment ▪ Provides oversight and strategic direction on behalf of the shareholders as authorized in the by-laws or State law ▪ Monitors corporate governance within an organization ▪ Approves financial statements ▪ Selects and evaluates CEO; approves appropriate compensation for CEO ▪ Evaluates attractiveness of and pay dividends ▪ Oversees share repurchase programs, recommend stock splits, etc. ▪ Recommends or discourages mergers and acquisitions
Vice President	▪ Second in command in an organization and has specific responsibilities depending on the needs of his or her organization as directed by the by-laws ▪ Assists in formulating and implementing the strategic plan that guides the direction of the business or their area of responsibility ▪ Leads, guides, directs, and evaluates the work of other executive leaders including assistant vice presidents, directors, and managers ▪ Achieves the organization's overall strategic goals and profitability requirements as determined by the strategic plans ▪ Assists creating, communicating, and implementing the organization's vision, mission, and overall direction ▪ In the President's absence, the Vice President acts in the role
Chief Operating Officer (COO)	▪ Responsible for the daily operations. ▪ Provides communication, leadership, and guides management as necessary to ensure that company has the proper operational controls, administrative and reporting procedures in place to effectively grow the organization ▪ Ensures effective communication with the President/CEO by keeping him/her informed of daily operations ▪ Ensures that operating objectives and standards of performance are understood by management and employees ▪ Ensures that Company complies with all applicable legal and regulatory requirements and, where appropriate, best practice to maximize the financial integrity of Company ▪ Ensures appropriate and satisfactory systems are in place for monitoring Company performance against planned and budgeted expectations
Limited Partner	▪ Generally does not have any kind of management responsibility. ▪ They are not material participants, strictly investors ▪ Share in profits and losses based on share of ownership
Member	▪ Similar to a stockholder in a corporation. Responsible for formation of the LLC and/or having owning interest in the LLC as designated in the Operating Agreement and/or State Law when there is no Operating Agreement ▪ Chooses a manager to manage the LLC ▪ Can also be the manager

Appendix B: Exclusion Resolutions

B.1 Highest Cleared Entity Noting Excluded Entity's Exclusion and Resolution to Exclude Parent Organization

I, *(Insert Full Name)*, the duly elected Secretary of *(Insert Name of Highest Cleared Entity)*, a corporation in the State of *(Insert Name of State)*, do hereby certify that the following is a true and complete copy of a resolution passed at a meeting of the Board of Directors of said Corporation, at which a quorum was present, duly called, and held
(Insert Month Day, Year).

BE IT RESOLVED that officials of *(Insert Name of Highest Tier Excluded Entity and any Intermediate Entities)*, the ultimate tier entity organization, or any of the intermediate tier entities of *(Insert Name and Address of Highest Cleared Entity)*, shall not require and shall not have access to classified information in the custody of *(Insert Name of Highest Cleared Entity)*, a subsidiary organization or any other facilities reporting to *(Insert Name of Highest Cleared Entity)* that require access to classified information.

BE IT FURTHER RESOLVED that *(Insert Name of Highest Cleared Entity)* hereby acknowledges the execution of a resolution by *(Insert Name and Address of Highest Excluded Entity)* whereby the Corporation, its officers and directors, as such, and intermediate entities will not require and will not have access to classified information in the custody of *(Insert Name of Highest Cleared Entity)*, a subsidiary corporation, and further that this action will not affect adversely the policies of said subsidiary involving the security and safeguarding of classified information or performance of classified contracts.

BE IT FURTHER RESOLVED that these actions of the Board of Directors of the *(Insert Name of Highest Cleared Entity)* are taken for the purpose of exempting the *(Insert Name of Highest Tier Excluded Entity and Intermediate Tiers)* from the necessity of being processed for a Facility Security Clearance equivalent to that held by the *(Insert Name of Highest Cleared Entity)* in conformity with the "National Industrial Security Program Operating Manual."

IN WITNESS WHEREOF I have hereunto set my hand and affixed the seal of *(Insert Name of Highest Cleared Entity)* this *(Insert Date)*.

_____**Signature**

Note: Two copies shall be furnished to the local DCSA Industrial Security field office with an original signature and corporate seal on each. One copy shall be furnished to the subsidiary. Both the highest tiered excluded entity and the highest cleared subsidiary must execute a "Certificate Pertaining to Foreign Interest" (SF 328).

If the parent is to be excluded from a higher category of classified information, the next to last paragraph should read "… from the necessity of having to be processed for a Facility Security Clearance equivalent to that held by the (Name of Subsidiary)."

B.2 Exclusion Resolution of Corporate Organization

I, *(Insert Full Name)*, the duly elected Secretary of *(Insert Name of Highest Tier Excluded Entity)*, a corporation organized in the State of *(Insert Name of State)*, located at *(Insert Address of Highest Tier Excluded Entity) do* hereby certify that the following is a true and complete copy of a resolution passed at a meeting of the Board of Directors of said Corporation, at which a quorum was present, duly called and held *(Insert Month Day, Year)*.

BE IT RESOLVED that *(Insert Name and Address of Highest Tier Excluded Entity and Intermediate Entities)*, its officers and directors, as such, will not require and will not have access to classified information in the custody of *(Insert Name of Highest Cleared Entity)*, or any other facilities reporting to *(Insert Name of Highest Cleared Entity)* that require access to classified information, and further that *(Insert Name of Highest Cleared Entity)*, has been delegated full authority to act completely independent of *(Insert Name of Highest Tier Excluded Entity and intermediate tiers)* in all matters that involve or relate to *(Insert Highest Cleared Entity's)* responsibility to perform on classified contracts, to include safeguarding classified information.

BE IT FURTHER RESOLVED that this action is taken for the purpose of exempting *(Insert Name of Highest Tier Excluded Entity and Intermediate Tiers)* from the necessity of being processed for a Facility Security Clearance (FCL) in conformity with the "National Industrial Security Program Operating Manual (NISPOM)." In lieu of a Facility Security Clearance, *(Insert Name of Highest Tier Excluded Entity)* will report any changed conditions, as defined in NISPOM 2-102, within the complete organizational structure that may impact the FCL eligibility of *(Insert Name of Highest Cleared Facility)*. Any changes that may impact FCL eligibility of *(Insert Name of Highest Cleared Facility)* will be disclosed to the Facility Security Officer at *(Insert Name of Highest Cleared Facility)* or in special circumstances, directly to the Defense Security Service.

IN WITNESS WHEREOF I have hereunto set my hand and affixed the seal of *(Insert Name of Company)* this *(Insert Date)*.

_____**Signature**

B.3 Exclusion Resolution for LLC Member (Organization)

I, *(Insert Full Name)*, the duly elected *(Management Official Title)* of *(Insert Name of LLC Member)*, a *(Type of Organization)* organized in the State of *(Insert Name of State)*, located at *(Insert Address of LLC Member)* do hereby certify that the following is a true and complete copy of a resolution passed at a meeting of the *(Type of Management B*oard*)* of *(Management Officials)* of said *(Type of Organization)*, at which a quorum was present, duly called and held *(Insert Month Day, Year)*.

BE IT RESOLVED that *(Insert Name and Address of LLC Member)*, its management officials, as such, will not require, shall not have, and can be effectively and formally excluded from access to classified information disclosed to *(Insert Name of subject LLC)*, a *Limited Liability Company*, and further that *(Insert Name of subject LLC)*, has been delegated full authority to act completely independent of *(Insert Name of LLC Member)* in all matters that involve or relate to *(Insert Name of subject LLC)'s* responsibility to safeguard information.

BE IT FURTHER RESOLVED that *(Insert Name and Address of LLC Member)*, is taken for the purpose of exempting the *(Insert Name of LLC Member)* from the necessity of being processed for a Facility Security Clearance in conformity with the "National Industrial Security Program Operating Manual."

Signature _____

Date_____
(Senior Management Official of LLC Member)

B.4 Exclusion Resolution for Certain Directors, Officers, and LLC Member (if Person)

I, (*Insert Full Name*), do hereby certify that I am (*Identify eligible KMP officer/position title*) of (*Insert Name of Corporation*), a (*Insert Corporation, Company*) organized and existing under the laws of the State of (*Insert Name of State*), and that the following is a true and correct copy of a resolution adopted by the Board of Directors, management board, or a similar type of executive body of the said (*Insert Corporation, Company*) at a meeting held at (*Insert Location*) on (*Insert Month, Day, Year*) at which time a quorum was present.

WHEREAS, current Department of Defense Regulations contain a provision making it mandatory that the Chairman of the Board, Senior Management Official and Facility Security Officer meet the requirements for eligibility for access to classified information established for a contractor facility security clearance; and

WHEREAS, said Department of Defense Regulations permit the exclusion from the personnel of the requirements for access to classified information of certain members of the Board of Directors and other officers, provided that this action is recorded in the corporate minutes.

NOW THEREFORE BE IT DECLARED that the Chairman of the Board, Senior Management Official and Facility Security Officer at the present time do possess, or will be processed for, the required eligibility for access to classified information; and

BE IT RESOLVED that in the future, when any individual enters upon any duties as Chairman of the Board, Senior Management Official and Facility Security Officer, such individual shall immediately make application for the required eligibility for access to classified information; and

BE IT RESOLVED AND DIRECTED that the following members of the Board of Directors and other officers or members shall not require, shall not have, and can be effectively and formally excluded from access to all **CLASSIFIED** information disclosed to the corporation/company and shall not affect adversely corporate/company policies or practices in the performance of classified contracts for the Department of Defense or the Government contracting activities (User Agencies) of the National Industrial Security Program.

NAME	TITLE

IN WITNESS WHEREOF I have hereunto set my hand and affixed the seal of (*Insert Name of Company*) this (*Insert Day/Month of Year*).

_____

Signature

Note: Two copies shall be furnished to the local DCSA Industrial Security field office with an original signature and corporate seal on each. One copy shall be furnished to the subsidiary. Both the highest excluded entity parent and highest cleared subsidiary must execute a "Certificate Pertaining to Foreign Interest" (SF 328).

Appendix C: Navigating the National Industrial Security Program (NISP) Risk Management Framework (RMF) Process

NISP Authorization Office

The NISP Authorization Office (NAO) as part of the DCSA Industrial Security Field Operations (IO Directorate) is responsible for the following:

- Risk management processes and procedures for classified information technology (IT) systems and architectures operated by cleared industry
- Management of the DCSA Assessment and Authorization process
- Oversight of authorized systems located at cleared contractor sites
- Technical oversite and policy for the cyber security workforce

Risk Management Support Elements

The risk management capability is composed of the primary elements:

- **Policy**
- **Process**
- **Cyber Security Workforce Professionals**

Policy

The overarching policy is derived from the following primary documents:

- **DOD 5220.72-M National Industrial Security Program Operating Manual (NISPOM)**
- **NISP SP 800-37 Rev _ Risk Management Framework for Information Systems and Organizations: a System Life Cycle Approach for Security and Privacy**
- **NIST SP 800-53 Rev _ Security and Privacy Controls for Federal Information Systems and Organizations**
- DAAPM – DCSA Assessment and Authorization Process Manual

The NIST Computer Security Resource Center (CSRC) contains numerous other policy documents referenced in the DAAPM. The library is located at: **https://csrc.nist.gov/**

The DoD directives library is available at: **https://www.esd.whs.mil/DD/**

The DCSA RMF Resource Center is located at: **https://www.DCSA.mil/ma/ctp/io/nao/rmf/**

Process

RMF Process Overview

The NAO risk management process is contained in the DAAPM *(Use link under the Policy Section)*. The RMF process overview is provided as described by the NIST SP 800-37. The NISP specific process and activities are contained in the DAAPM. New NISP participants should read both of these policies documents to support RMF implementation. For RMF process questions contact your assigned Information Systems Security Professional or the DCSA RMF mailbox *(See RMF Resources)*.

Cyber Security Workforce Professionals

The IO cyber security workforce is composed of

- **Authorization Officials (AO)**
- **Information Systems Security Professional Team Leads (ISSP TL)**
- **Information Systems Security Professionals (ISSP)**

The DAAPM contains the specifics on roles and responsibilities for each of these billets. Additionally, the Industry cyber security roles and responsibilities for RMF process support are contained in the process manual. The roles are

- **Information System Security Manager (ISSM)**
- **Information System Security Officer (ISSO)**

Alphabetized NISP RMF Resources

The following resource links are provided:

Resource	Location
DCSA Assessment and Authorization Process Manual	https://www.DCSA.mil/Portals/69/documents/io/rmf/DCSA_Assessment_and_Authorization_Process_Manual_Version_2.0.pdf
DISA eMASS Training	https://rmfks.osd.mil/rmf/Pages/default.aspx
DoD Cyber Awareness Challenge	https://iase.disa.mil/eta/Pages/index.aspx
NISP eMASS	https://emass-nisp.csd.disa.mil/
NISP eMASS Job Aids	https://www.DCSA.mil/ma/ctp/io/nao/rmf/ 1. Go to NISP eMASS Information and Resource Center Diagram 2. Click on Training 3. eMASS Training Resources appear below.
NIST Computer Security Resource Center	https://csrc.nist.gov/
RMF Knowledge Service	https://rmfks.osd.mil/rmf/Pages/default.aspx

Questions and Concerns

DAAPM Questions contact: DCSA.quanticoDCSA-hq.mbx.odaa@mail.mil

NISP eMASS Questions contact: DCSA.quantico.DCSA.mbx.emass@mail.mil

Appendix D: Sample 328/441 Guides / Sample Orgainization Chart

D.1 DD Form 441 Completion Sample

DEPARTMENT OF DEFENSE SECURITY AGREEMENT

OMB No. 0704-0194
OMB approval expires Sept 30, 2019

PLEASE DO NOT RETURN YOUR FORM TO THE ORGANIZATION IN THE PARAGRAPH BELOW. RETURN COMPLETED FORM TO YOUR RESPECTIVE COGNIZANT SECURITY OFFICE.

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 the Department of Defense, Washington Headquarters Services, Executive Services Directorate, Directives Division, Office of Information Management, 4800 Mark Center Drive, East Tower, Suite 03F09, Alexandria, VA 22350-3100 (0704-0194). 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. DISCLOSURE: Voluntary, however, if the form is not provided, a facility clearance cannot be issued.

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

DO NOT FILL IN THE DATE

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

ENTER COMPANY'S LEGAL NAME *(hereinafter called the Contractor)*, which is:

(1) A LMITED LIABILITY COMPANY organized and existing under the laws of the state of STATE ORGANIZED IN
(Enter type of business entity, e.g., Corporation, Limited Liability Company, etc.)

(2) a partnership consisting of LEAVE BLANK

(3) an individual trading as LEAVE BLANK

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

ENTER COMPANY'S FULL ADDRESS

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 contracts for the purchase of supplies or services, 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 classified information; and

WHEREAS, the parties desire to define and specify 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 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), which is made hereto and made a part of this agreement, subject, however, to (i) 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 particular business and necessary procedures thereunder.

(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

DD FORM 441, JAN 2017 PF

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 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.

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

THE UNITED STATES OF AMERICA

By _____
(Signature of Authorized Government Representative)

_____
(Typed Name of Authorized Government Representative)

_____
(Typed Name of Authorized Government Agency)

ENTER COMPANY'S LEGAL NAME
(Typed Name of Contractor Entering Agreement)

WITNESS

WITNESS' SIGNATURE AND DATE
(Signature and Date)

WITNESS' TYPED NAME

NOTE: The witness must be a person who personally observed the Contractor Representative sign this form. The witness cannot be the same person who signs this form as the Government Representative. The name of the witness should be typed or printed under the witness' signature and date.

By SMO'S SIGNATURE
(Signature of Authorized Contractor Representative)

SMO'S TYPED NAME
(Typed Name of Authorized Contractor Representative)

SMO'S TITLE
(Title of Authorized Contractor Representative)

COMPANY'S STREE ADDRESS
(Contractor Address)

COMPANY'S CITY, STATE, ZIP
(Contractor Address)

By executing this form, the Contractor Representative certifies that he or she is the SMO'S TITLE of the business entity identified above, and has the authority to bind the business entity to the terms of this agreement.

DD FORM 441 (BACK), JAN 2017

Reset

D.2 SF 328 Certification Guide

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:

THIS DATE MUST MATCH THE WITNESS DATE
(Date Certified)

WITNESS' SIGNATURE AND DATE
(Signature and Date)

By SMO'S SIGNATURE
(Signature of Authorized Contractor Representative)

WITNESS' TYPED NAME

SMO'S TYPED NAME
(Typed Name of Contractor)

NOTE: The witness must be a person who personally observed the Contractor Representative sign this form. The witness cannot be the same person who accepts this form as the Government Representative. The name of the witness should be typed or printed under the witness' signature and date.

SMO'S TITLE
(Title of Authorized Contractor Representative)

COMPANY'S FULL ADDRESS
(Address)

By executing this form, the Contractor Representative certifies that he or she is the SMO'S TITLE of the business entity identified above, and has the authority to bind the business entity to the terms of this agreement.

Reset

STANDARD FORM 328 (REV. 3/2017) **BACK**

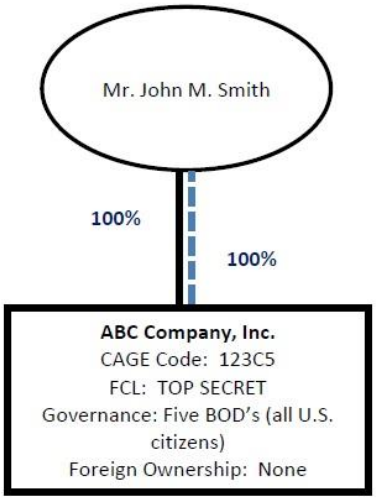
D.2.1 SF-328 Instructions

SF328_Instructions.pdf

(Attached to PDF Handbook)

D.3 Sample Organization Chart

ORGANIZATIONAL CHART (Sample – Sole Proprietorship)



Appendix E: FCL Package Submission Checklist

This checklist is not all inclusive for the successful submission of an FCL package. This checklist is intended to assist facilities in avoiding common reasons for rejection of the FCL package.

Basic Information and Documentation

1. Please confirm all required documentation is provided for the appropriate business structure.
2. Please do not "package" the documentation and upload under multiple document types
3. On the basic information tab, please confirm the business structure selected is correct.
4. Please included all prior legal company names and prior legal addresses.
5. Please confirm the principal place of business listed in SAM, the Secretary of State website(s), and provided business documentation match or the discrepancy is addressed.
6. Please provide documentation reflecting business structure conversion, if appropriate.
7. Please confirm the facility is registered to conduct business within the state even if organized in different state (i.e. principal address/located in Virginia, but organized in Delaware).
8. All shares of stock accounted for, including un-issued shares.
9. The legal organization chart should reflect the owners/members of the facility. Please include (but not limited to): name, percentage of ownership, membership, or stocks held, and all appointed titles; for companies include address and CAGE code if applicable.

SF-328 and DD-441

10. On the SF-328, please provide detailed replies to any questions answered "yes."
11. SF-328 & DD-441 signed by the Senior Management Official, witnessed and dated the same day.
12. On the SF-328 & DD-441, the titles for Authorized Contractor Representative and the certifying official match.
13. On the DD-441, please ensure is date field is blank on the first page.
14. On the DD-441 signature block, enter the facility name on the "typed name of contractor entering agreement" line.

KMP Information and KMP List

15. Please confirm the Personal Identifiable Information (PII) (spelling of names, Social Security Number, date of birth, etc.) is correct.
16. Please provide the FSO and ITPSO appointment letter(s) confirming the individual(s) is an employee of the company and US citizen as required per NISPOM 2-103c.
17. Please provide the FSO appointment date on the KMP list.
18. On the KMP list, please indicate each individual once and include all roles and titles associated with that individual.
19. Please confirm the provided roles and titles indicated are supported by the documentation (Operating Agreement/By-laws etc).
20. Please identify any positions required by the business documents and are currently not filled are listed as VACANT.
21. Please confirm one Senior Management Official (SMO) is identified on the KMP list. The SMO is NOT a position which can be appointed, but is determined based on the company's governance documents. (NOTE: there are some rare circumstances in which there may be more than one SMO).
22. Please provide the exclusion resolution for any non-required KMPs (unless access to classified information is required in support of the contractual work).
23. Ensure Proof of citizenship for all required KMPs is uploaded to the FCL package.
24. Additional companies are not included on the KMP list. In cases of a JV, a company (member) will not be added to the KMP list, rather the company's representative will be added to the KMP list.
25. Please provide the documentation reflecting the election/appointment of the Officers/Board Members, etc.