



Facility Clearance Orientation Handbook

Defense Counterintelligence and Security Agency

Industrial Security
Entity Vetting Directorate

July 2026



Table of Contents

Points of Contact.....	4
Resources Page	5
Index.....	7
Welcome Message	8
1.0 Overview of the NISP	9
1.1 FCL Lifecycle	11
1.2 FCL Roadmap.....	12
2.0 Facility Security Officer (FSO) Responsibilities and Deadlines	13
2.1 Before Sponsorship Acceptance.....	13
2.2 After Sponsorship Acceptance	14
2.3 Post-FCL Determination	15
3.0 FCL Process Overview	17
3.1 FCL Package Submission	18
3.2 FCL Upgrade Information	18
3.3 Expedite Request Guidelines.....	19
3.4 FCL Adjudication.....	20
3.5 FCL Appeals Process.....	24
3.5.1 The FCL Denial, Revocation, and Appeals Process:.....	24
4.0 FCL Package Submission Guidance	27
4.1 Key Management Personnel (KMP) Identification	27
4.1.1 Required (Essential) KMP verses Excluded KMP.....	27
4.1.2 Senior Management Official (SMO).....	28
4.1.3 Facility Security Officer (FSO)	28
4.1.4 Insider Threat Program Senior Official (ITPSO).....	28
4.1.5 Other KMP	29
4.2 Business Structure-Specific KMP and Required Documentation.....	29
4.3 Special Purpose Entities	31
4.3.1 Branch Office/Division	31
4.3.2 Joint Venture (JV)	32
4.3.3 Tribal Entity.....	33
4.4 Upgrades.....	33
4.5 Additional Guidance on FCL Package Documentation.....	33
5.0 Excluded Parent Process	36
5.1 Sponsored Facility and Excluded Parent Definitions and Responsibilities	37
5.2 Excluded Parent Workflow Example	38
6.0 Accounts and Systems	39
7.0 Tools and Training	41
7.1 FSO Training	41



7.2 Insider Threat Program Training.....	41
Appendix A: Common KMP Authorities by Position	43
Appendix B: Sample DD-441, SF-328, and SF-328 Signature Pages	45
B.1 DD Form 441 Completion Sample	45
B.2 SF-328 Certification	46
B.3 SF-328 Certification (Signature Block) Example	47
Appendix C: Sample Organizational Charts	48
C.1 Sole Proprietorship.....	48
C.2 LLC (Member-Managed)	49
C.3 LLC (Manager-Managed).....	50
C.4 Corporation.....	51
C.5 Joint Venture.....	52
C.6 Complex Business Structure.....	53
C.7 University Structure	54
C.8 Branch Offices	55
Appendix D: FCL Package Common Errors List.....	56
Appendix E: FCL Package RFI Process	58
Appendix F: FCL Discontinuation.....	60
Appendix G: PKI/ECA – access to NCAISS and NISS	61
Appendix H: Common Acronyms	62
Appendix I: Proposed Exclusion Resolution Templates.....	64
I.1 Highest Cleared Entity Noting Excluded Entity’s Exclusion and Resolution to Exclude Parent Organization	64
I.2 Exclusion Resolution of Corporate Organization.....	65
I.3 Exclusion Resolution for LLC Member (Organization).....	66
I.4 Exclusion Resolution for Certain Directors, Officers, and LLC Member or Manager (if Person).....	67



Points of Contact

Facility Clearance Process, Update Requests, and Package-Related Questions

- **Entity Vetting Directorate Knowledge Center**
 - Email: dcsa.quantico.mbx.ev-vtd@mail.mil
 - Phone: (878) 274-2000 (option 2, then 1)

National Industrial Security System (NISS)-Related Questions or Issues

- **NISS Technical Line**
Phone: (878) 274-2000 (option 2, then 3)

National Background Investigation Services (NBIS) eAPP (electronic application)

- **For applicant support with eAPP, contact the Applicant Knowledge Center (AKC)**
 - Email: dcsa.boyers.dcsa.mbx.applicant-knowledge-center@mail.mil
 - Phone: (878) 274-5091
 - Hours 6:00 a.m. – 5:00 p.m. EST

DoD Help Desk Information

- **DoD PKI Help Desk (DISA)**
 - Email: disa.gsd.maops@mail.mil
 - Phone: (844) 347-2457 Option 1,3,4
- **DoD PKE Help Desk (DISA)**
 - Email: dodpke@mail.mil
- **ECA Program Office (DISA)**
 - Email: disa.meade.mae.list.pkieca@mail.mil
- **CAC Support (DMDC)**
 - <http://www.cac.mil/common-access-card/developer-resources/>
 - Email: cacsupport@mail.mil
- **Vendor ECA Support – Check DoD Cyber Exchange Site for Current Vendor List**
 - <https://public.cyber.mil/pki-pke/help/>
- **IdenTrust, Inc.**
 - <http://www.identrust.com/certificates/eca/index.html>
 - Email: helpdesk@identrust.com
 - Phone: (888) 882-1104
- **WidePoint - Operational Research Consultants, Inc. (ORC)**
 - <http://www.eca.orc.com/>
 - Email: wscs.helpdesk@widepoint.com
 - Phone: (800) 816-5548

Post-FCL and DCSA Field-Related Questions or Concerns

- **DCSA Field Offices and Contact Information**
 - <https://www.dcsa.mil/Industrial-Security/Field-Locations/>



Resources Page

Policy

- 32 CFR Part 117, National Industrial Security Program Operating Manual (NISPOM Rule)
 - <https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117>
- DTM 24-004
 - https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dtm/DTM-24-004.PDF?ver=xjHWilUsiMyXVOt7kR3t_g%3d%3d (note: expiration date extended)
- DoD Manual 5220.32
 - Volume 1
(<https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/522032v1.PDF?ver=1BFNVqOKXaqdXcO618H-yg%3D%3D>)
 - Volume 2
(https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/522032v2.PDF?ver=6r6Wq0aBhS44uQvw8Vne_w%3D%3D)
- 48 CFR 52.204-18, Commercial and Government Entity Code Maintenance.
 - <https://www.ecfr.gov/current/title-48/section-52.204-18>
 - https://www.acquisition.gov/far/52.204-16#FAR_52_204_16_d3091e43

Forms

- Exclusion Resolutions
- DD-441
 - <https://www.esd.whs.mil/Portals/54/Documents/DD/forms/dd/dd0441.pdf>
- DD-441-1
 - <https://www.esd.whs.mil/Portals/54/Documents/DD/forms/dd/dd0441-1.pdf>
- SF-328
 - <https://www.gsa.gov/reference/forms/certificate-pertaining-to-foreign-interests>
- SF-86
 - https://www.opm.gov/forms/pdf_fill/sf86.pdf
- DD254
 - [https://www.esd.whs.mil/Directives/forms/dd0001_0499/DD254/#:~:text=Form%20Number%3A%20DD%20254&text=Title%3A%20Department%20of%20Defense%20Contract,Security%20Classification%20Specification%20\(Download%20Instructions\)&text=Edition%20Date%3A%2004%2F01%2F2018_r](https://www.esd.whs.mil/Directives/forms/dd0001_0499/DD254/#:~:text=Form%20Number%3A%20DD%20254&text=Title%3A%20Department%20of%20Defense%20Contract,Security%20Classification%20Specification%20(Download%20Instructions)&text=Edition%20Date%3A%2004%2F01%2F2018_r)

Training and Guidance

- FCL Orientation Videos – Under Construction
- NCAISS/NISS User Guide
 - https://www.dcsa.mil/Portals/128/Documents/IS/DCSA_NCAISS_PS3_NCAISS_User_Guide.pdf
- NISS Industry Onboarding
 - <https://www.dcsa.mil/Systems-Applications/National-Industrial-Security-System-NISS/NISS-Industry-Onboarding/>



Systems

- Defense Logistics Agency (DLA)
 - <https://www.dla.mil/Vendor-Information-Hub/Table-of-Contents/Details/Article/3606127/registration-renewal-and-cage-creation-in-system-for-award-management-sam/#Signing%20Up%20VS%20Registering>
- System for Award Management (SAM)
 - <https://sam.gov/>
- Defense Information System for Security (DISS)
 - <https://www.dcsa.mil/Systems-Applications/Defense-Information-System-for-Security-DISS/>
- Fingerprint service providers
 - <https://www.dcsa.mil/is/swft/swftresources/>
- NCAISS
 - <https://www.dcsa.mil/Systems-Applications/National-Industrial-Security-Program-NISP-Central-Access-Information-Security-System-NCAISS/>
- NISS
 - <https://www.dcsa.mil/Systems-Applications/National-Industrial-Security-System-NISS/>

Obtaining Public Key Infrastructure (PKI) or External Certification Authority (ECA)

PKI and ECA Resources

- PKI Interoperability Website:
 - <https://public.cyber.mil/pki-pke/interoperability/>
- ECA PKI Support Organizations:
 - <https://public.cyber.mil/pki-pke/help/>
- ECA
 - <https://public.cyber.mil/eca/>
- DoD ECA X.509 Certificate Policy
 - https://dl.dod.cyber.mil/wp-content/uploads/eca/pdf/unclass-eca_cp.pdf
- Frequently Asked Questions
 - <https://www.cyber.mil/faqs>



Index

- Adjudication: [20-24](#)
- Appeals: [24-26](#)
- Branch: [31-32](#), [33-34](#), [56](#)
- Corporation: [28](#), [30](#), [32-33](#), [44-45](#), [52](#), [64](#)
- Discontinuation: [14](#), [59-61](#)
- Excluded Parent (XP): [36-38](#), [47](#), [57](#)
- Facility Security Officer (FSO): [13-19](#), [27-35](#), [39-43](#)
- FCL Lifecycle: [11](#)
- FCL Process Roadmap: [12](#)
- Insider Threat Program Senior Official (ITPSO): [17](#), [27-30](#), [42-43](#)
- Key Management Personnel (KMP): [9](#), [14-18](#), [23](#), [27-35](#), [44-45](#), [57-58](#)
- Legal Organizational Chart: [49-56](#)
- Limited Liability Company (LLC): [29-30](#), [32-34](#), [44-45](#), [50-51](#)
- Limited Liability Partnership: [31](#)
- Limited Partnership/General Partnership: [31](#), [44](#), [54](#)
- Parent Entity: [9-10](#), [27](#), [30](#), [34-38](#), [47](#), [58](#)
- Senior Management Official (SMO): [17](#), [27-36](#), [42](#), [57-58](#)
- SF-328: [5](#), [18-19](#), [29-30](#), [33-37](#), [47-48](#), [57-58](#)
- Ultimate Excluded Parent: [33-38](#)
- University/College (Academic Institution): [28](#), [31](#), [55](#)
- Upgrade: [14](#), [18-19](#), [28-29](#), [33](#), [59-60](#)



Welcome Message

On behalf of the Defense Counterintelligence and Security Agency (DCSA), welcome to the facility clearance (FCL) process. Your facility has recently been sponsored for access to classified information by a government contracting activity (GCA), cleared contractor, or foreign government under the National Industrial Security Program (NISP) for performance on a classified government contract. DCSA will be overseeing your FCL and security program as the cognizant security office (CSO) administering the NISP on behalf of the Department of War (DoW) and 35 other federal agencies (<https://www.dcsa.mil/Industrial-Security/National-Industrial-Security-Program-Oversight/NISP-Signatories/>).

DCSA considers its relationship with industry as a vital partnership in the safeguarding of U.S. national security. We are committed to supporting your facility throughout and beyond the FCL process while under DoW cognizance. The importance of your organization in the protection of U.S. national security interests cannot be overstated - whether your facility provides critical hardware, innovative software, essential services, or any other contribution to DoW or the defense industrial base - you play a crucial role in supporting and enabling U.S. warfighters. This immense responsibility requires a proactive, unwavering commitment to security across the entire enterprise.

The requirements, restrictions, and other safeguards which cleared facilities must implement are outlined in 32 Code of Federal Regulations (CFR) Part 117, National Industrial Security Program Operating Manual (NISPOM) Rule (<https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117>) . This Handbook does not replace the NISPOM Rule and it is your organization's responsibility to meticulously review the sections and chapters of the NISPOM Rule applicable to your security program to fully understand your obligations under the security agreement your facility is about to execute with the U.S. Government (DD Form 441, <https://www.esd.whs.mil/Portals/54/Documents/DD/forms/dd/dd0441.pdf>).

DCSA looks forward to partnering with you and your facility. Please do not hesitate to reach out to the Knowledge Center or your Industrial Security Representative as you begin navigating the FCL process.

Matthew Kitman
Deputy Assistant Director
Entity Vetting Directorate



1.0 Overview of the NISP

The NISP was established by Executive Order 12829, as amended, in January 1993 for the protection of classified information. The NISP applies to all executive branch departments and agencies, and to all cleared contractor facilities located in the United States, its territories, and possessions. The Secretary of War has entered into agreements with other federal departments and agencies to provide industrial security services, current listing is available at: <https://www.dcsa.mil/Industrial-Security/National-Industrial-Security-Program-Oversight/NISP-Signatories/>.

Participation is voluntary, but access to classified information will not be permitted unless a facility agrees to, and abides by, NISP requirements. When your facility receives its FCL, it will be subject to provisions of the 32 Code of Federal Regulations (CFR) Part 117, National Industrial Security Program Operating Manual (NISPOM Rule) <https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117>. You are expected to review and become familiar with 32 CFR Part 117. The FCL Orientation Handbook is not intended to replace 32 CFR Part 117, it is simply a guide to inform and assist with navigating the FCL process.

An FCL is an administrative determination that a facility is eligible to access classified information. The process begins with a government agency, or a prime contractor submits a sponsorship in the National Industrial Security System (NISS) database. Following acceptance of the sponsorship, the Facility Security Officer (FSO) will receive a welcome email directing the facility to obtain a NISS account and provide documentation. This welcome email officially starts the clock on several critical, time-sensitive actions. This FCL Orientation handbook is your comprehensive guide, designed to walk you through each stage of this process and help ensure a successful outcome.

Phase	Required Action & Timeline
1. PKI Token Application	The appointed FSO must immediately apply for a Public Key Infrastructure (PKI) token . This is required for National Industrial Security System (NISS) access and can take several weeks to arrive.
2. FCL Package Submission	The facility has 20 days to submit its initial FCL package. This must include key business documents and identify Key Management Personnel (KMP), such as the Senior Management Official (SMO), FSO, and Insider Threat Program Senior Official (ITPSO).
3. Personnel Security (PCL)	Essential KMP must be processed for a Personnel Security Clearance (PCL) at or above the requested FCL level and complete the SF-86 via eAPP or successor system. Non-essential KMP must be formally excluded.
4. DCSA Coordination	Throughout the entire process, the FSO must remain highly responsive and readily available to answer any inquiries from DCSA.
5. Final Adjudication	DCSA evaluates the complete package for risks—including Foreign Ownership, Control, or Influence (FOCI)—to ensure granting the



clearance aligns with U.S. national security interests.

The classification levels in the NISP are CONFIDENTIAL, SECRET, and TOP SECRET. Your facility's FCL level is based on the classified contract requirements, the solicitation, [DD-254](#), security classification letter, or other accepted documentation. DCSA may issue an interim FCL prior to issuance of the final FCL. For an interim FCL, DCSA must first validate that there is no unmitigated FOCI, and the essential key management personnel (KMP) - individuals required to be cleared in connection with the FCL - have eligibility determinations at the interim level or higher. A final FCL (also known as an Entity Eligibility Determination) cannot be issued until the first four stages of the [FCL lifecycle](#) have been completed and all essential KMP are cleared at the final level of the requested FCL.

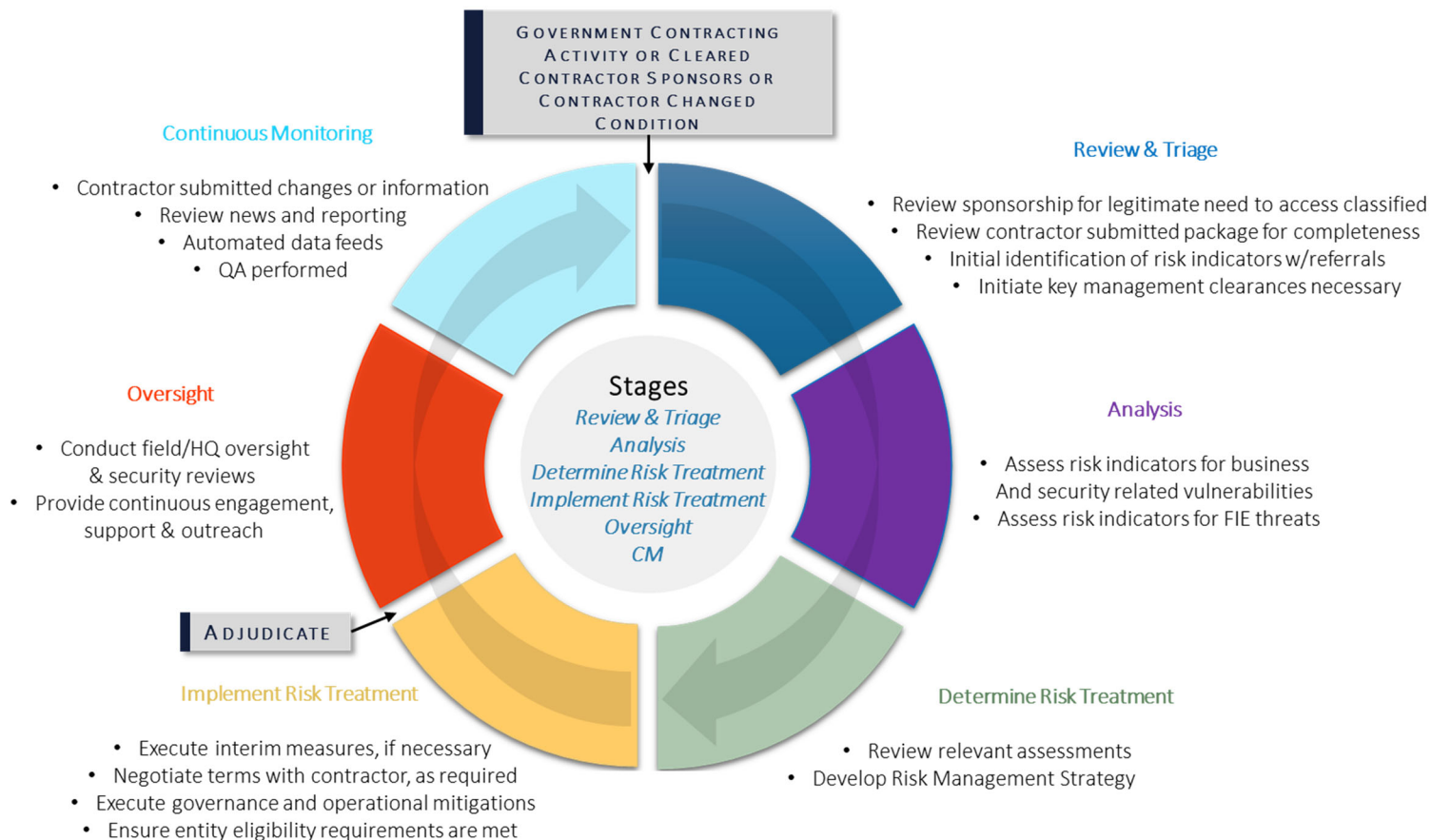
Please note, essential KMP are required to hold the same level personnel security clearance (PCL) or higher as the FCL before the final FCL can be issued. PCL background investigation and adjudication processing timelines may result in delays issuing the final FCL. Non-essential KMP, who are not required to hold PCLs in connection with the FCL, must be excluded via Exclusion Resolution.

If there are other facilities within the same legal structure, such as a parent or member entities, a decision will be made to clear or exclude these entities by DCSA during the initial review of the FCL Package in NISS. Additionally, when FOCI is present, the timelines for processing the FCL will likely be extended due to the required review, analysis, and potential implementation of FOCI risk treatment.



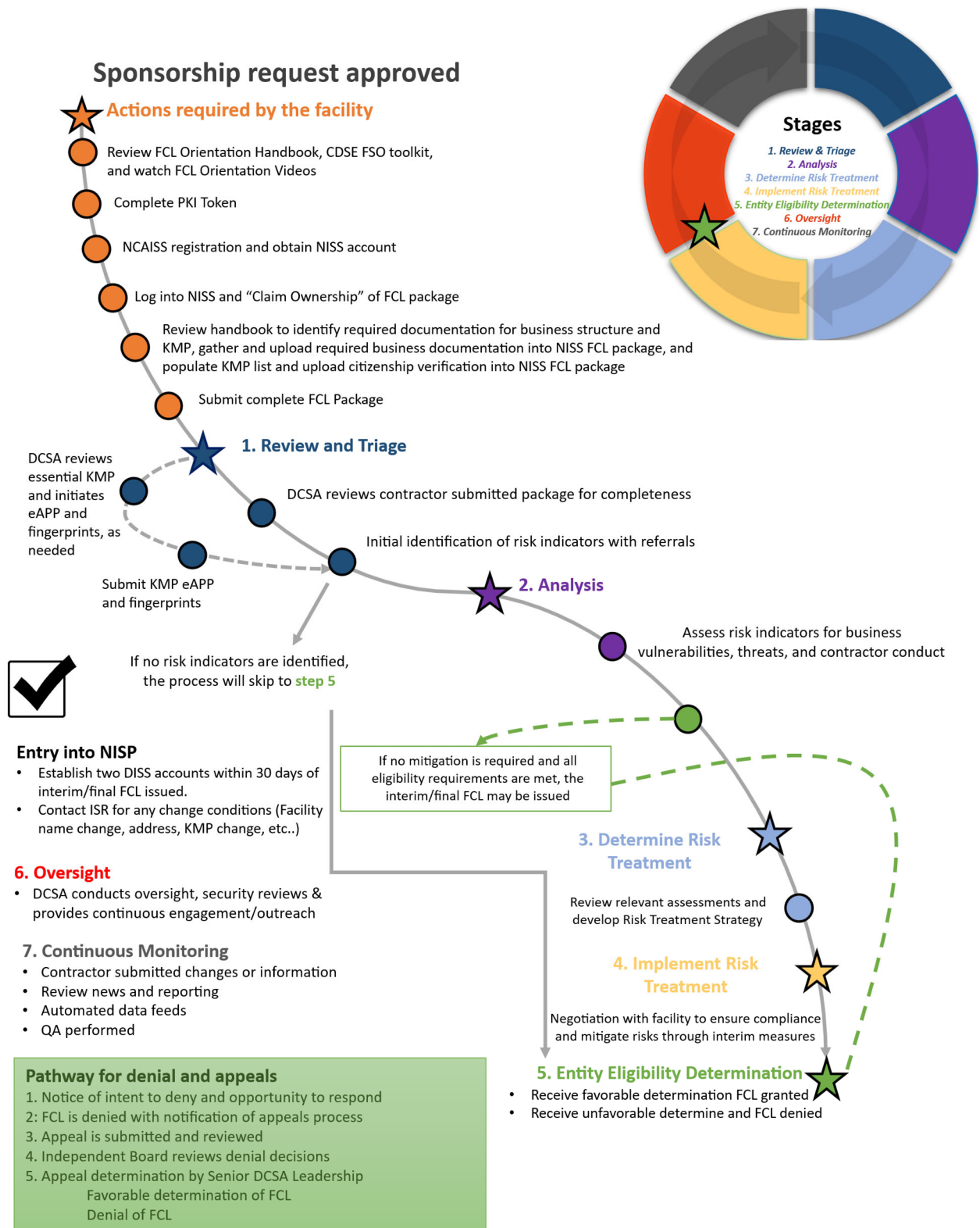
1.1 FCL Lifecycle

The FCL processing times are unique to each company. This orientation handbook is designed to guide you through a “right the first time” submission to minimize delays and focus on company readiness. Ensuring first-time accuracy on your forms and providing swift responses to DCSA inquiries are the most critical factors within your control to accelerate your package.





1.2 FCL Roadmap





2.0 Facility Security Officer (FSO) Responsibilities and Deadlines

Welcome to the National Industrial Security Program (NISP). As a Facility Security Officer (FSO), you are central to your organization's security, acting as the primary liaison to DCSA to ensure regulatory compliance.

Be prepared and available to discuss your facility's business structure, personnel, and promptly respond to questions from DCSA. Throughout this period, your ability to answer questions and work with other parts of your organization to collect and provide information is crucial.

Immediate Action: Apply for Your [Public Key Infrastructure \(PKI\)](#) or External Certification Authority (ECA) token.

You must apply for your PKI token; it is essential for secure authentication to access NISS. The process to acquire a PKI token can take several weeks.

2.1 Before Sponsorship Acceptance

Once DCSA accepts the FCL sponsorship in NISS, the FSO will have strict deadlines for document submission. The information below can help you get ahead of the requirements and be prepared if you know your facility will be awarded a classified contract:

- Anyone conducting business with the U.S. government is required to have and maintain a Commercial and Government Entity (CAGE) code through the Defense Logistics Agency (DLA) CAGE (DLA CAGE) database through the life of the contracts, and prime contract holders are required to be registered with [SAM.gov](#) (48 CFR 52.204-18 and [FAR 52.204-18](#)). Once an account is created in DLA CAGE, a Unique Entity ID will be issued, and a CAGE code will be generated for them. Additional guidance on how to receive a CAGE code and register with DLA CAGE and SAM can be found at [DLA](#).
- To submit the documentation DCSA requires, the FSO will first need to ensure they have a PKI or ECA to access the NISP Central Access Information Security System (NCAISS), the system housing the National Industrial Security System (NISS). NISS is the system-of-record where all FCL-related information is housed and processed. It can take two weeks or more to obtain an ECA, so it is best practice to get the process started early. PKIs take longer to process and typically require a Common Access Card. See the [Resources Page](#) for more information on PKI certificates and a list of DoD approved PKI vendors.
- In addition to the FCL Orientation Handbook, DCSA's FCL Orientation Videos provide a detailed, narrated guide to the FCL process, including associated milestones and deadlines. You can watch them as many times as needed for reference. <https://www.dcsa.mil/Industrial-Security/Entity-Vetting-Facility-Clearances-FOCI/Facility-Clearances/> are a detailed, narrated guide that will walk through the FCL process. DCSA strongly encourages FSOs to take the necessary time to view these videos. Along with the FCL Orientation Handbook, these videos provide all the information needed to meet all requirements for the FCL process. After you have **thoroughly** reviewed the information contained in the videos, handbook, and attached documents, please direct any questions to the [DCSA Entity Vetting Directorate Knowledge Center](#). Direct any NISS technical questions to the [NISS Technical Line](#).



2.2 After Sponsorship Acceptance

Once DCSA accepts the sponsorship, the timeline begins. During the first 20 days following acceptance of the FCL sponsorship request, it is your responsibility to identify your facility's [business structure](#) and provide required documentation and forms in NISS.

There are two deadlines during the FCL process:

1. Required legal documentation and DCSA forms **must be submitted** through an initial FCL package in NISS within **20 days** of receiving the NISS-generated Welcome E-mail (Day 1).
 - It is the FSO's responsibility to ensure all required documentation is submitted within the allotted timeframe, and provided documentation is complete and accurate. Failure to do so may result in FCL processing delays or discontinuation of the facility's FCL request.
 - Once the documentation is submitted, the FSO should ensure they are available to respond to calls or emails from DCSA requesting additional information or clarification.
 - DCSA implements an approach, wherein the facility has two chances to address any discrepancies, or missing information preventing DCSA from processing the FCL package. Should the facility fail to provide the requested information within the two allotted attempts, DCSA will discontinue the process, **EVEN IF** it is before the 20-day deadline. Please see [Appendix F](#) for further guidance.
2. Upon receipt of the FCL Package, DCSA will review the PCL status of the essential KMP. Any essential KMP without a PCL, or a PCL at a lower level than the FCL, will be initiated for an investigation request by DCSA. Once the background investigation(s) are initiated, the FSO will receive an email from DCSA with instructions and a due date for the investigation submission and fingerprints.
 - Please include the personal email address for all essential KMP on the KMP tab within the NISS FCL package. This information is needed to send the required documentation to start the security clearance eligibility process.
 - For an [FCL Upgrade](#), the FSO is responsible for initiating background investigation(s), for its essential KMP including updated fingerprints. DCSA will provide a courtesy email to the FSO upon completion of the Review and Triage Stage of the Upgrade FCL Package, which will include a suspense date for SF-86 via eAPP, or successor system, and fingerprint submittal.

There are two categories of individuals who must be submitted for a PCL during the sponsorship acceptance process:

1. **Essential Key Management Personnel (KMP):** Essential KMP who do not have the appropriate PCL eligibility must complete the SF-86 form electronically via eAPP and submit electronic fingerprints, or successor systems.
 - a. **The Process:** Once the FCL package is submitted, DCSA will email these individuals directly with instructions to access eAPP (or its successor system)..
 - b. **How to prepare:** All KMP should familiarize themselves with the requirements of



holding a PCL. Because paper forms are not accepted, KMP should download the SF-86 PDF to gather their background information offline before logging in.

https://www.opm.gov/forms/pdf_fill/sf86.pdf.

2. **Negotiator or Mission Critical Employee:** DCSA will process PCLs for individuals identified as the negotiator, or a mission critical employee who is not a KMP, at the request of the GCA.
 - a. **The Process:** The GCA will provide written notification to DCSA which will include the individuals' name and position. DCSA will contact the facility to obtain necessary information for the individuals to start the PCL process.
 - b. **How to Prepare:** Identify which personnel may require a PCL during the pre-award phase, or at the start of the contract due to knowledge or a skillset that is necessary immediately to support the mission. Per the DoD Manual 5220.32, Volume 1, Section 4.11 *National Industrial Security Program: Industrial Security Procedures for Government Activities*,
<https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/522032v1.PDF?ver=1BFNVqOKXaqdXcO618H-yg%3D%3D>, The negotiator typically requires

Electronic fingerprints must be submitted to DCSA via 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, another cleared facility or use a third-party service provider. A list of third-party service providers can be found on DCSA's website <https://www.dcsa.mil/is/swft/swftresources/>. Please note that the locations listed are headquarters offices and do not indicate all the areas the provider serves. Many providers have nationwide locations or offer fingerprint card conversion services, in which a hard copy fingerprint card can be mailed for conversion to the proper electronic format and uploaded to SWFT. Whatever method or provider you use, **you should verify that the fingerprints are being submitted to DCSA via SWFT**, as many organizations submit fingerprints to other agencies through other systems.

2.3 Post-FCL Determination

Once DCSA issues an FCL, the facility and KMP are required to comply with 32 CFR Part 117, [National Industrial Security Program Operating Manual \(NISPOM Rule\)](https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117) <https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117> and implement an effective security program. Your facility's assigned Industrial Security Representative (ISR) will reach out within 120 days of the FCL being issued to conduct a brief assessment of your facility's compliance with 32 CFR Part 117 requirements and implementation of the facility security program and insider threat program.

The FCL initial orientation meeting is conducted by an ISR assigned from the local field office **after** the FCL is granted. Please be prepared to discuss the following topics with the ISR:

- Facility's [32 CFR Part 117](https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117) <https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117> requirements
- [Facility's Security Program](https://www.cdse.edu/Training/Toolkits/FSO-Toolkit/) <https://www.cdse.edu/Training/Toolkits/FSO-Toolkit/>
- [Facility's Insider Threat Program](https://www.cdse.edu/Training/Toolkits/Insider-Threat-Toolkit/) <https://www.cdse.edu/Training/Toolkits/Insider-Threat-Toolkit/>
- When requested, provide KMP U.S. citizenship verification (accepted documentation for citizenship is located at: <https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117>)



[I/subchapter-D/part-117/section-117.10#p-117.10\(c\)](#)



3.0 FCL Process Overview

A Facility Clearance (FCL), also known as an entity eligibility determination, is an administrative approval for a company to access classified information. To obtain an FCL, a company must prove a legitimate need for access, be organized and located within the United States or its territories and have a history of lawful business conduct. Furthermore, essential key management personnel (KMP) must hold appropriate personnel security clearances, and the company must not be under any unmitigated foreign ownership, control, or influence. The process formally begins when a sponsorship request is accepted and a welcome email is sent, which directs the company to register in the National Industrial Security System (NISS).

The NISPOM Rule defines an FCL 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 (32 CFR 117.3(b))

[https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117/section-117.3#p-117.3\(b\)](https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117/section-117.3#p-117.3(b)) An FCL may also be called an entity eligibility determination (32 CFR 117.3(b)) [https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117/section-117.3#p-117.3\(b\)](https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117/section-117.3#p-117.3(b)) though FCL is the common term.

To obtain an FCL, a facility must meet the eligibility requirements listed in [32 CFR 117.9\(c\)](https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117/section-117.9) (<https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117/section-117.9>) and meet PCL requirements for essential KMP (32 CFR 117.9 ;<https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117/section-117.9>). It is important to understand to be favorably adjudicated for FCL, a facility must meet the eligibility requirements below and must not pose an unacceptable risk to national security interest.

- Have a legitimate need for the requested FCL, either in terms of access to classified, or other accepted situations.
- Be organized and existing under the of the United States, one of the fifty States, the District of Columbia, or an organized U.S. territory (Guam, Commonwealth of the Northern Marianas Islands, Commonwealth of Puerto Rico, and the U.S. Virgin Islands); or American Indian or Alaska Native tribe under whose laws the entity is chartered has been formally acknowledged by the Assistant Secretary—Indian Affairs, of the U.S. Department of the Interior.
- Be located in the United States or its territories.
- Have a record of integrity and lawful conduct in business dealings.
- The SMO, FSO, ITPSO, and other essential KMPs hold a PCL at the same or higher level than the FCL, and not be excluded from participating in USG contracts or agreements IAW [§ 117.7\(b\)\(1\)](https://www.ecfr.gov/current/title-32/section-117.7#p-117.7(b)(1)) [https://www.ecfr.gov/current/title-32/section-117.7#p-117.7\(b\)\(1\)](https://www.ecfr.gov/current/title-32/section-117.7#p-117.7(b)(1)) through [§ 117.7\(b\)\(3\)](https://www.ecfr.gov/current/title-32/section-117.7#p-117.7(b)(3)) [https://www.ecfr.gov/current/title-32/section-117.7#p-117.7\(b\)\(3\)](https://www.ecfr.gov/current/title-32/section-117.7#p-117.7(b)(3)).
 - Note: a requirement to have background investigations to meet position or contract requirements or for access to a physical space(s) does not meet the eligibility requirements for an FCL. Please ensure you understand how your facility meets this requirement as verification will be emphasized throughout the [FCL lifecycle](#).
- Not be under FOCI to such a degree that access to classified information would be inconsistent with national interest, in the judgement of DCSA as representative of the CSA.
- Maintain sufficient authorized and cleared employees to manage and implement the requirements of the NISP.
- Does not pose an unacceptable risk to national security interest, in the judgement of DCSA as



representative of the CSA.

- Meet all the requirements governing access to classified information.

Once the sponsorship request is accepted, a welcome email will be sent automatically. This is Day 1 of this process. The welcome email identifies specific deadlines for your facility and guides you to register for an account within the NISS, DoD's system of record for tracking FCL-related actions and information for entities in the NISP.

3.1 FCL Package Submission

Once all the required business documents are collected and reviewed, upload into NISS under the "Submit My FCL Package." To populate the package and upload documents, you will need to have a NISS account and be using one of the following roles:

- FSO
- Alternate FSO
- Other Security Staff – This role is for anyone else tasked to perform security-related work supporting the FSO or alternate FSO

Once the FCL package has been populated with all required information and documents, submit the FCL package for DCSA's review. Guidance for submission of the FCL package is located in NISS under the "Access the External Knowledge Base" quick link. Prior to submitting the FCL package, review the applicable Business Structure Slick Sheet and the FCL Package Common Errors List found in [Appendix D](#). This will assist in avoiding many common mistakes, which result in the FCL package being returned for revision and will delay the FCL process. After you have submitted the FCL package, ensure the FCL Package status in NISS has been updated to "Submitted."

3.2 FCL Upgrade Information

If your facility has been sponsored to upgrade the FCL level, the FCL process is largely the same with some key differences. The facility should have an established NISS account, as well as primary and alternate [Defense Information System for Security \(DISS\)](#) <https://www.dcsa.mil/Systems-Applications/Defense-Information-System-for-Security-DISS/> account holders. The facility will submit an FCL package to the assigned ISR and annotate any changes. Note: All FCL upgrades will remain assigned to the local field office, and the FCL packages will be reviewed by the facility's currently assigned ISR. DCSA will continue to oversee the FCL process and triage for risk indicators.

While completing the FCL upgrade package, the KMP list must be verified or updated in accordance with any changes the facility has made. The KMP may need to submit a new or upgrade PCL request and fingerprints to upgrade their PCLs, if they are not already cleared at the same or higher level than the FCL upgrade. One key difference in the FCL process for an upgrade is that the **FSO is responsible for initiating the upgrade PCL investigation request for the KMP**, and the alternate DISS account holder will initiate the investigation request for the FSO. The upgrade PCL investigation requests should be initiated once the FSO has submitted the FCL package in NISS. Prompt submission of the FCL package will prevent any



delays in processing times.

It is recommended that when submitting the NISS upgrade FCL package, the FSO reviews and/or updates the SF-328 to ensure it is accurate. The facility's FCL package will once again be reviewed, triaged, and analyzed for any potential FOCI.

3.3 Expedite Request Guidelines

GCAs may submit a request to expedite via email to Entity Vetting the FCL process at any point for a specific facility if a delay significantly impacts the classified contract. This request allows DCSA to evaluate and potentially prioritize the FCL processing based on the urgency and impact of the situation.

The expedite request must be **submitted on the official letterhead of the requesting GCA responsible for the classified contract** and must include the following:

Impact Statement:

The GCA should provide a detailed explanation of the potential impact on the classified contract's cost, schedule, and performance if the FCL process is not expedited. This explanation must address any performance consequences that could jeopardize mission success or national security.

Contract Information:

1. The contract number and relevant details about the classified effort
2. A description of the facility's role and responsibilities under the contract
3. Identify the facility by name and CAGE code

Rationale for Expedite:

1. Justification for why the FCL process must be prioritized
2. Any supporting documentation that provides context for the urgency of processing

Once complete, the letterhead memorandum must be signed by an authorized GCA representative and submitted through the Sponsorship Request via NISS. Once submitted, DCSA will evaluate each request on a case-by-case basis. Submission does not guarantee prioritization. The decision to prioritize FCL processing will depend on:

1. The validity and urgency of the stated impacts
2. Resource availability and competing priorities
3. Submission of an expedite request does not guarantee prioritization, but incomplete or vague submissions are likely to result in delays or denials



3.4 FCL Adjudication

The FCL adjudicative process involves a comprehensive evaluation of the facility's suitability for access to classified information. The FCL eligibility requirements indicate the facility must not pose an unacceptable risk to national security interests, as stated in [the Eligibility Requirements https://www.ecfr.gov/current/title-32/part-117#p-117.9\(c\)](https://www.ecfr.gov/current/title-32/part-117#p-117.9(c)). As part of this determination, DCSA will consider all available information and weigh various factors, including allegiance to the United States and foreign influence. All doubts will be resolved in favor of national security. The final determination is based on a reasonable judgment of whether granting or continuing the FCL is clearly consistent with the interests of national security.

Category A - Ownership

The Concern: Foreign ownership and interests, including, but not limited to business, financial, and property interests, are a national security concern if they result in divided allegiance. There may be a national security concern if circumstances in which a facility may be manipulated or persuaded to help a foreign person, group, organization, or government in a way inconsistent with U.S. interests or susceptible to pressure or coercion by any foreign interest.

Examples that could raise security concerns include but not limited to:

- Foreign Ownership:
 - o A foreign interest: (A) has the power to control or influence issues affecting the entity's management or operations and/or (B) shares people, processes, or information with the facility that could result in unauthorized access to classified information or adversely affect the performance of a classified contract or agreement.
 - o Ownership or control, in whole or in part, by a foreign government.
- Unvetted New Ownership:
 - o A facility merged with or was acquired by another facility and that facility is not eligible for an FCL or cannot be effectively excluded from access to classified operations at the cleared facility.
 - o Shared people, processes, or information with the new owner that could result in unauthorized access to classified information or have an adverse impact on the performance of classified contracts.
- Other factors that would indicate or demonstrate a capability on the part of foreign interests to control or influence the operations or management of the business organization.
 - o Cleared facility personnel report to foreign citizens.
 - o The facility or its management has affiliations with foreign state-owned entities or organizations affiliated with a foreign government.



Category B - Business Operations

The Concern: Business activities that may allow an unvetted facility access to classified, sensitive, or proprietary information at the U.S. facility.

Examples that could raise security concerns include but not limited to:

- Joint Ventures & Partnerships:
 - o The facility or its controlling interest has formed a joint venture with a foreign facility or organization.
 - o The facility or its controlling interest has formed a joint venture with an uncleared facility or organization.
- Supply Chain Concerns:
 - o The facility or its controlling interest uses foreign sources for parts, components, research and development (R&D), assembly, or software coding in critical defense programs or technology.
 - o The facility or its controlling interests own or operate subsidiary supply-chain nodes, i.e. factories, warehouses, or distribution centers in a country of special concern.
 - o Reliance on foreign-produced hardware and software that may include design vulnerabilities that could provide foreign actors with access to a facility's networks and information.
 - o Reliance on foreign entities to provide critical parts, components, assembly, coding, R&D, or manufacturing that could affect the quality or availability of the facility's products or services.
- Legal Business Status:
 - o The facility or its controlling interest is forfeited, not in good standing, suspended or dissolved.
- Unreported FCL Change Conditions:
 - o The facility has undergone changes to their business structure to include changes which resulted in foreign ownership, control, or influence that would adversely affect their ability to continue to work on classified contracts.

Category C - Financials

The Concern: Failure to satisfy debts and meet financial obligations may indicate poor financial outlook, a lack of judgment or an unwillingness to abide by rules and regulations, all of which can raise questions about a facility's viability and ability to protect classified or sensitive information. Financial distress can also be caused or exacerbated by, and thus can be a possible indicator of, other issues of security concern. A facility that is financially overextending is at greater risk of insolvency, targeting, pressure, accepting risky foreign investments and insider threats.



Examples that could raise security concerns include but not limited to:

- Bankruptcy:
 - o The facility or its controlling interest has filed for bankruptcy.
- Excessive or Foreign Debt:
 - o Excessive indebtedness, significant negative cash flow, a history of late payments or of non-payment, or other negative financial indicators.
 - o Reliance on foreign entities for financing.
- Negative Financial Health:
 - o The facility or its controlling interest is found to be financially insolvent.
 - o The facility or its controlling interest is at risk of default.
 - o A history of not meeting financial obligations.
 - o Failure to file annual Federal, state, or local income tax returns or failure to pay annual Federal, state, or local income tax as required.
- Foreign Investment:
 - o The facility or its controlling interest has received direct or indirect investment from a foreign entity.
 - o The facility or its controlling interest has received private investment from a foreign entity.
- Suspicious Financial Activity:
 - o Susceptibility or a willingness to compromise sensitive and classified information and technologies in exchange for money or investments to keep the facility viable.
 - o Sudden unexplained reversal of a negative financial situation or repayment of large debts.
 - o Deceptive or illegal financial practices such as filing deceptive loan statements and other intentional financial breaches of trust.
 - o Conducting business or financial activities inside a sanctioned country.
 - o Receiving loans from individuals or non-financial institutions.

Category D - Personnel Considerations

The Concern: Criminal activity creates doubt about an individual's judgment, reliability, and/or trustworthiness and which may be predictive of their willingness or ability to protect U.S. national security. By its very nature it calls into question a person's ability or willingness to comply with laws, rules, and regulations. A pattern of conduct, including those for relatively minor offenses, may, when taken in combination cast doubt on the individual's judgment, reliability, or trustworthiness. Failure to adhere to the laws of the U.S. may be relevant if the violation of law is harmful to stated U.S. interests. An individual who engages in acts against the U.S. or provides support or encouragement to those who do has already demonstrated a willingness to compromise national security.



Examples that could raise security concerns include but not limited to:

- Foreign Management and Influence:
 - o A foreign national is in a position of control that allows them to influence facility management or operations through direct or indirect affiliation.
 - o Cleared facility key management personnel (KMP) has ties to foreign subsidiaries or foreign facilities, including serving as members of boards or leadership teams.
 - o The facility KMP are employed on behalf of a foreign government, including foreign intelligence service, foreign military service, foreign diplomatic service, or foreign political office.
- Criminal Activity:
 - o Facility KMP is engaged in criminal activity, i.e. fraud, embezzlement, money laundering and insider trading.
 - o Facility KMP is involved in unauthorized technology transfer.
 - o Facility KMP is involved in economic and government espionage against U.S. targets.
 - o Facility KMP is engaged in conduct that is indicative of untrustworthy or unreliability to include breach of client confidentiality, release of proprietary information, unauthorized release of sensitive corporate or government protected information.
- Suspicious Associations:
 - o Facility KMP associate or engage with a terrorist group or extremist movement (foreign or domestic).
 - o Facility KMP are found in watch lists in connection with the decisions of a regulatory body for international trade.
 - o Facility KMP associate or engage with organizations advocating the overthrow of the U.S. Government.
 - o Facility KMP are associated with the threat of violence, against a current or former Government official or Agency.
- Personnel Security Clearance Eligibility Concerns:
 - o Essential KMP are uncleared or not cleared to the level of the FCL.
 - o Personnel reassignments are occurring to circumvent personnel security clearance requirements tied to the facility, even though the individuals' roles and responsibilities remain largely unchanged.

Category E - Business Conduct

The Concern: Facilities must have a record of integrity and lawful conduct in their business dealings and not pose an unacceptable risk to national security interest.

Examples that could raise security concerns include but not limited to:

- Criminal Activity:
 - o The facility or its controlling interest is engaged in criminal activity.
- Sanctions/Restrictions:



- The facility or its controlling interest is found on watch lists in connection with the decisions of a regulatory body for international trade.
 - The facility or its controlling interest is doing business with an organization found on watch lists in connection with the decisions of a regulatory body for international trade.
 - The facility or its controlling interest is subject to international or U.S. sanctions.
- Suspicious Associations:
 - The facility or its controlling interest, associate or engage with a terrorist group or extremist movement.
 - The facility or its controlling interest, associate or engage with organizations advocating the overthrow of the U.S. Government.
 - The facility or its controlling interest, associate or engage with criminal organizations.
- NISP Compliance:
 - The facility failed to protect classified, proprietary, or sensitive information (e.g., sharing of protected information, admission of mishandling protected information).
 - The facility failed to report a compromise or mishandling of classified information.
 - The facility or its controlling interest has been excluded or debarred from performing on government contracts.
 - Gross negligence or lax security practices.
 - Failure to comply with rules or regulations that result in damage to national security, regardless of whether it was deliberate or negligent.
 - Unwillingness to comply or fix known security vulnerabilities.
 - Record of non-compliance with pertinent U.S. laws, regulations, and contracts.

3.5 FCL Appeals Process

If a facility's Facility Clearance is denied or revoked, a written Statement of Reason will be provided. The facility can challenge the decision by submitting a detailed response and opportunity to discuss with government officials. The final determination is based upon the best interest of national security.

3.5.1 The FCL Denial, Revocation, and Appeals Process:

Step 1 – “Intent to Deny or Revoke Package” includes Notice of Intent to Deny or Revoke, Statement of Reasons (SOR) and Opportunity to Respond

The “Intent to Revoke Package” is comprised of three documents, which 1) notifies a company of DCSA's intent to revoke their FCL, 2) lists security concerns within a Statement of Reasons (SOR) which support grounds for revocation, and 3) provides the company an opportunity to respond with clarifying information.



The package is sent to the company's personnel listed under the firm's profile within DCSA's National Industrial Security System (NISS) and consists of the following:

1. Notice of Intent to Revoke/Deny Memorandum:
 - Provides a summary of the security concerns and supporting risk information.
 - Instructions for responding to the SOR.
 - A list and description of the information in the decision to Deny/Revoke FCL determination.
2. SOR:
 - Provides the company written notice for the Denial/Revocation.
 - Accompanies the Notice of Intent to Deny/Revoke.
 - Identifies the reasons based on the FCL Adjudicative Guidelines for the intent to Deny/Revoke.
3. Opportunity to Respond:
 - Gives company the opportunity to provide clarifying information, plans to remedy, correction of inaccurate information, or any other information or substantive changes to the factors listed in the SOR within 15 calendar days of the date of the Notice of Intent to Revoke/Deny Memorandum.
 - Failure to respond within 15 calendar days will result in the immediate move to issue a denial or revocation. The specific calendar due date will be clearly stated.

Step 2 – Final Determination is made with notification of Appeals Rights

When a facility clearance is denied or revoked, the company will receive a notification explaining their right to appeal the decision within 30 calendar days, including the procedures and timelines for doing so.

Purpose of notification of appeals rights include:

Ensures Due Process:

- The right to be notified of adverse actions and to respond.
- Provides a mechanism for challenging adverse decisions.
- Ensure that facility clearance decisions are made in accordance with fair procedures and legal requirements.

Promotes Fairness and Transparency:

- Ensures impartial review of facility clearance appeals.
- Fosters objective consideration of all evidence presented during the appeal process.
- Guarantees companies the opportunity to present their case fully and openly during the appeal.

Step 3 – Appeal Submission

The facility's appeal must clearly and comprehensively state the specific grounds for challenging the decision. In response DCSA must ensure decisions are consistent with overarching DoD policy and legal frameworks for an appeals process.

Examples of appeal submission may include:

Formal Written Document:

- Cite specific information or documents that contradict the agency's findings. Be precise and avoid generalizations.



- Identify the specific regulation, policy, or legal standard that the agency allegedly misapplied or violated.
- Describe the specific corrective actions and enhanced security measures that the facility has implemented to mitigate the agency's concerns.

Request for Meeting with DCSA to Verbally Present Appeal:

- Facility can request to meet with DCSA representatives to state its case.
- Provides an opportunity to respond to follow up or amplifying questions in real-time to aid in the decision-making process.

Step 4 – FCL Denial/Revocation Independent Review Board

The primary purpose is to provide an independent review of DCSA's preliminary decision to deny or revoke an FCL which will be submitted to the Associate Director, Industrial Security for a final determination. This helps ensure fairness, impartiality, and adherence to established procedures.

Purpose of the review board:

Objective Assessment:

- The board is comprised of impartial members from different DCSA mission areas.
- Thorough review of all relevant documents, including the documentation to support the recommendation, SOR, the facility's response, witness statements, and any other evidence submitted by either party.
- The review board will make a recommendation to the Associate Director, Industrial Security, after reviewing all relevant information related to the proposed denial or revocation.
- The Associate Director, Industrial Security will consider the review board's recommendation and make a final determination whether to accept the board's recommendation and issue a notification letter to the facility.

Clear and Transparent Procedures:

- If the intent to deny or revoke is upheld, the notification letter will include as much detail as possible. Some details may be redacted if supporting information is classified.

Step 5 – Appeal Determinations

Appeals decisions will be escalated to the Associate Director for Industrial Security. The Associate Director will review the appeal and will either uphold the initial decision or choose to reinstate or grant the FCL with conditions.

Notification to the Contractor:

- A detailed explanation of why the appeal was or was not granted.
- If the denial or revocation was based on specific security deficiencies, the facility should take steps to correct those deficiencies if they are interested in pursuing an FCL in the future.
- The Associate Director, Industrial Security will consider the review board's recommendation and make a final determination whether to accept the board's recommendation and issue a notification letter to the facility.



4.0 FCL Package Submission Guidance

This section details the required business structure documents and KMP list identification to submit in the facility's FCL Package in NISS. Please review the Checklist and [Appendix D](#) Common Errors for assistance to ensure a complete and accurate FCL package is submitted in NISS.

DCSA does not solely look at the in-process facility when evaluating for an entity eligibility determination/FCL. DCSA must evaluate the entire business organizational structure in totality. In many cases, if there is a parent facility involved, or multiple tiers to the structure, documentation must be submitted for the highest U.S. facility in the organizational structure, as well as the facility which is in process for an FCL. DCSA will review the entire structure's ownership and control to identify and assess risk. If there are multiple tiers, DCSA will need to identify any/all stakeholders with 5 percent or greater interest in the in-process facility on a fully diluted basis. This is increasingly important if your organization structure has limited partnerships, or private equity involvement. For a list of documents required to be submitted for your organization's parent facility, please see the [business structure](#) required documents that pertain to your parent facility.

For specific questions on what documentation may need submitted for your facility, please contact the EV Knowledge Center.

4.1 Key Management Personnel (KMP) Identification

4.1.1 Required (Essential) KMP versus Excluded KMP

A required or essential KMP is an individual who holds a position of ownership, control or influence to such a degree the individual in the position must obtain PCL in accordance with the FCL at the same or higher level. The 32 CFR, Part 117 specifically identifies the SMO, FSO and ITPSO as KMP require the PCL in connection with the FCL. Other KMP will be determined as required based upon the circumstance of each entity. Typically, required KMP includes but are not limited to the positions of: Chairperson of the Board (and all variations), Board of Directors (when there is not a chairperson, or the chairperson position rotates), CEO, President, Member, Manager, sole owner, and similar roles or positions as determined by DCSA.

Excluded KMP are individuals who hold positions of ownership, control, or influence which is limited or negated to such a degree the individual in the position does not require a PCL in accordance with the FCL. This individual must be identified on the KMP list, but an exclusion resolution can be exercised to effectively restrict the individual's access to classified information or issues involving the safeguarding of classified information. Typically, excluded KMP includes but are not limited to the positions of: Directors (when there is a chairperson, or the chairperson position does not rotate), Vice-President, Treasurer, Secretary, Chief Financial Officer, and similar roles or positions as determined by DCSA. **NOTE:** Excluded KMP may require a PCL in support of the classified contract effort.

For an excluded KMP who requires access to classified information in performance of the classified contract, the SMO must provide a letter on company letterhead, stating the



KMP can be effectively and formally excluded from adversely affecting policies and procedures of the facility and that the individual requires a PCL eligibility to access classified information in the course of assigned duties and provide support on the classified contract.

4.1.2 Senior Management Official (SMO)

Senior Management Official (SMO) is the facility official responsible for the entity policy and strategy. The SMO is an entity employee occupying a position in the entity with **ultimate** authority over the facility's operations and the authority to direct actions necessary for the safeguarding of classified information in the facility. This includes the authority to direct actions necessary to safeguard classified information when the access to classified information by the facility's employees is solely at other contractor facilities or USG locations. This position cannot be temporarily excluded during the initial or upgrade FCL process.

The SMO is the individual with the ultimate authority to act and make decisions on behalf of the entity facility; not an individual who has direct oversight of the classified contracting efforts. The responsibilities of the SMO are outlined in [32 CFR 117.7\(b\)\(2\)](https://www.ecfr.gov/current/title-32/part-117#p-117.7(b)(2)) [https://www.ecfr.gov/current/title-32/part-117#p-117.7\(b\)\(2\)](https://www.ecfr.gov/current/title-32/part-117#p-117.7(b)(2)). The SMO must hold an active PCL at the same or higher level as the FCL and may not be excluded from participating in USG contracts or agreements.

DCSA will make the final determination of the facility's SMO based upon the entity's business structure, ownership, control and provided governance documentation. Typically, a SMO is the individual who holds the position of managing-member or manager (for a limited liability companies), CEO or President (if there is no CEO) (for a corporation), and president or Chancellor at a University/College.

4.1.3 Facility Security Officer (FSO)

Facility Security Officer (FSO) is the individual who will supervise and direct security measures necessary for implementing the applicable requirements of this rule and the related USG security requirements to ensure the protection of classified information [32 CFR 117.7\(b\)\(3\)\(i\)](https://www.ecfr.gov/current/title-32/part-117#p-117.7(b)(3)(i)) [https://www.ecfr.gov/current/title-32/part-117#p-117.7\(b\)\(3\)\(i\)](https://www.ecfr.gov/current/title-32/part-117#p-117.7(b)(3)(i)). The FSO is appointed by the SMO, must be a U.S. citizen employee of the facility, must hold an active PCL at the same or higher level than the FCL and not be excluded from participating in USG contracts or agreements, and complete the required trainings [32 CFR 117.9\(d\)\(1\)](https://www.ecfr.gov/current/title-32/part-117#p-117.9(d)(1)) [https://www.ecfr.gov/current/title-32/part-117#p-117.9\(d\)\(1\)](https://www.ecfr.gov/current/title-32/part-117#p-117.9(d)(1)), [32 CFR 117.9\(c\)\(5\)](https://www.ecfr.gov/current/title-32/part-117#p-117.9(c)(5)) [https://www.ecfr.gov/current/title-32/part-117#p-117.9\(c\)\(5\)](https://www.ecfr.gov/current/title-32/part-117#p-117.9(c)(5)). This position cannot be temporarily excluded during the initial, upgrade, or change condition process. [32 CFR 117.9\(g\)\(1\)](https://www.ecfr.gov/current/title-32/part-117#p-117.9(g)(1)) [https://www.ecfr.gov/current/title-32/part-117#p-117.9\(g\)\(1\)](https://www.ecfr.gov/current/title-32/part-117#p-117.9(g)(1))

4.1.4 Insider Threat Program Senior Official (ITPSO)

Insider Threat Program Senior Official (ITPSO) is the individual who will establish and execute an insider threat program at the facility. [32 CFR 117.7\(b\)\(4\)](https://www.ecfr.gov/current/title-32/part-117#p-117.7(b)(4)) [https://www.ecfr.gov/current/title-32/part-117#p-117.7\(b\)\(4\)](https://www.ecfr.gov/current/title-32/part-117#p-117.7(b)(4)). The ITPSO is appointed by the SMO, must be a U.S. citizen employee of the facility, must hold an active PCL at the same or higher level than the FCL and not be excluded from participating in USG



An entity facility may establish a “family-wide” insider threat program with one senior official appointed as the ITPSO. Each cleared entity within the “family” must appoint the individual as ITPSO. The ITPSO will provide an implementation plan for executing the insider threat program across the entity “family.”

In addition to the SMO, FSO, and ITPSO, an entity will include on the KMP list all other individuals who holds majority ownership, hold an appointed position in accordance with the entity's governance documentation (such as officers, directors, etc.), has the authority to directly or indirectly control or influence management or operations decision affecting the classified contract performance, or other individuals as determined necessary by DCSA. Please see [Appendix A](#) for Common KMP Authorities by Position.

All business structures have unique considerations when it comes to KMP and required documentation, however the information identified below is the standard requirements across all business structures. Subsequent sections on each business structure will identify unique requirements in addition to these standard requirements. When creating a KMP list, refrain from using titles which are only used in practice, and which are not reflected in the corporate governance documentation. KMP should also provide personal email addresses for creation of eAPP accounts.



Business Structure	Required Information & Documentation	KMP List Identification
1. All	- State formation documentation - Business License - Meeting Minutes# (if applicable) - Please provide appointments of directors, managers, officers, or any other individual identified in the corporate governance documentation - Fictitious Name Certificate (if applicable) - Legal Organizational Chart - See Appendix C of FCL Orientation Handbook - Ownership and control MUST each be identified by percentage - FSO & ITPSO listed in NISS. - Signed and witnessed DD-441 - Signed and witnessed SF-328 - Citizenship Verification - Required for KMP who do not possess PCL - Personal email address for all KMP who must be processed for a PCL (this is for creation of an eAPP account) - Exclusion Resolutions (if applicable) - See DCSA website https://www.dcsa.mil/Systems-Applications/National-Industrial-Security-System-NISS/NISS-Industry-Onboarding/ - Exclusion resolutions are subject to DCSA concurrence - Does your facility have a Parent Company? - Parent Company = Entity holding >50% interest in your facility (ownership or control) - If yes, refer to section 7 of the FCL Orientation Handbook for detailed guidance # May be known at the facility by a different name, such as Memorandum for Record (MFR), Board Resolution, or other name(s).	- Senior Management Official (SMO)* - Facility Security Officer (FSO)* - Insider Threat Program Senior Official (ITPSO)* - Board chairperson(s)* - Where the entity has a managing board and a chair is identified - Rotating chairpersons must all be cleared - In the absence of a chairperson, enough directors to form a quorum must be cleared - Any other individuals determined to have unilateral binding or management authority over the facility* - Officer positions identified in the corporate governance documentation - Directors or similar for managing board <i>*Denotes position required to be cleared in connection with the FCL IAW company governance documents.</i>
2. Limited Liability Company	- All required documentation in row 1 above - Certificate of Formation/Articles of Organization - Operating Agreement (OA) - If not identified in the OA, please provide a list of ownership/membership - If the state does not require an OA and the facility does not have one, a signed document on company letterhead must be provided identifying, at a minimum, ownership, management, and control	- All required KMP in row 1 above - If manager-managed: Manager(s)* - LLCs with a board of managers (or similar term) will follow the same requirements for a chairperson identified in row 1 - If member-managed: Member(s)* - Persons only on the KMP list - Members of member-managed LLCs must be cleared, including if the members are other entities
3. Corporation	- All required documentation in row 1 above - Articles of Incorporation - By-Laws - Stock Ledger/Capitalization Table - All shares and classes of stock MUST be accounted for - Capitalization table is preferred - For publicly traded corporations: most recent Securities and Exchange Commission Filings (10K/Proxy Statement and any subsequent 13D/F filings.	All required KMP in row 1 above



4. Academic Institution	1. All required documentation in row 1 above 2. Charter a. If the charter does not describe how the organization is run or managed, a separate document, such as by-laws or a constitution, must be provided	1. All required KMP in row 1 above
5. General Partnership	1. All required documentation in row 1 above 2. Partnership agreement a. Not all states require partnership agreements, however DCSA requires documentation detailing the ownership, control, and management of the partnership 3. DCSA required documentation demonstrating the general partnership is legally organized and existing and is not solely a partnership by agreement	1. All required KMP in row 1 above 2. General partners* 3. Management or executive committee members (if applicable)*
6. Limited Partnership	1. All required documentation in row 1 above 2. Partnership agreement a. Not all states require partnership agreements, however DCSA requires documentation detailing the ownership (partnership interest), control, and management of the partnership 3. Certificate of limited partnership	1. All required KMP in row 1 above 2. General partners* 3. Management or executive committee members (if applicable)* 4. Any other partners may be processed for a PCL based on their role in the partnership
7. Limited Liability Partnership	1. All required documentation in row 1 above 2. Partnership agreement a. Not all states require partnership agreements, however DCSA requires documentation detailing the ownership (partnership interest), control, and management of the partnership 3. Certificate of Formation or Articles of Organization 4. Any other documentation outlining ownership, control, and management of the partnership	1. All required KMP in row 1 above 2. Managing partners* 3. Any other partners may be processed for a PCL based on their role in the partnership
8. Sole Proprietorship	1. All required documentation in row 1 above 2. DCSA requires documentation demonstrating that the sole proprietorship is legally organized and exists as a sole proprietorship and identifying the jurisdiction whose laws it is operating under.	1. All required KMP in row 1 above 2. Sole proprietor*

4.3 Special Purpose Entities

4.3.1 Branch Office/Division

A branch office or division is a separate location for an existing legal company, referred to as a multiple facility organization (MFO). Because a branch office is part of the same legal entity as its home office (HOF), they must have the same legal name. In most cases, only the HOF requires an FCL. A branch office or division only requires a separate FCL issued by DCSA if there's a requirement to safeguard collateral classified information within that office. If no safeguarding is required at the branch office, administrative security requirements, such as PCL processing and training, are handled by the HOF.

For branch offices requiring an FCL, the HOF must always be cleared to the same or a higher level as the branch office. The majority of the legal business documents and forms required are provided by the home office, therefore the FCL package requirements for a branch office or division are minimal.



Please ensure the “Business Structure” field on the Basic Information tab of the FCL Package is marked as “Branch or Division”. The required documents include DD441-1; citizenship verification for KMP who do not already possess a PCL (birth certificate, passport); a complete legal organizational chart (must include all branch/divisions); Meeting Minutes (specific to the branch/division only). Please note the HOF SMO is required to certify all legal documents for the branch/division office.

The KMP list for a branch office has the only type of KMP list in which the individuals listed are not required to be designated in the legal business documents. The SMO with Ultimate Authority must retain accountability of the security program, IAW 32 CFR 117.7(b)(2)(v) ([https://www.ecfr.gov/current/title-32/part-117#p-117.7\(b\)\(2\)\(v\)](https://www.ecfr.gov/current/title-32/part-117#p-117.7(b)(2)(v))).

Finally, the SMO, FSO, ITPSO (as defined in 32 CFR 117.7[b], [https://www.ecfr.gov/current/title-32/part-117#p-117.7\(b\)](https://www.ecfr.gov/current/title-32/part-117#p-117.7(b))) must be identified on the KMP list and must be cleared or processed for a PCL at the level of the FCL requested.

4.3.2 Joint Venture (JV)

A joint venture (JV) is not a business structure. It is an association of two or persons or business (frequently called venturers) engaged in a defined project with all parties contributing assets and efforts, and sharing in the management, profits and losses, all in accordance with the terms of an agreement among the parties. There are two common forms of JVs, a JV created as a legal entity and a "joint venture by contract.” DTM 24-004, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dtm/DTM-24-004.PDF?ver=xjHWiUsiMyXVOt7kR3t_g%3d%3d, dated July 19, 2024, provides clarification on when JVs with DoD contracts should be processed for FCLs. An FCL is not required for a “covered JV,” which is defined as those in which all venturers maintain active FCLs granted by DCSA.

A JV formed as a legal entity may be organized in the form of a partnership, corporation, or limited liability company. The JV will be processed for an FCL in accordance with the procedures that apply to the appropriate business structure. For example, if the JV documentation shows that the joint venture is an LLC, the JV will be processed for an FCL as an LLC. This is necessary to meet eligibility requirements IAW 32 CFR 117.9(c), [https://www.ecfr.gov/current/title-32/part-117#p-117.9\(c\)](https://www.ecfr.gov/current/title-32/part-117#p-117.9(c)), an organization must be legally organized and existing in the United States. Note that a JV by contract who is not formed as a legal registered business facility is not eligible for an FCL.

Business records and KMP requirements are determined by the type of business structure (LLC, Corporation, Partnership, etc.). Required business documents for a JV should include the formation documentation (demonstrating that the JV is legally organized and existing); JV Agreement (may be incorporated in an LLC Operating Agreement); governance documentation that is specific to the business structure (i.e., Operating Agreement, By-Laws, or Partnership Agreement).

NOTE: An FCL is not required for a joint venture (JV) in the NISP, provided it qualifies as a **covered JV** under DTM 24-004, [https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dtm/DTM-24-](https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dtm/DTM-24-004)



[004.PDF?ver=xjHWilUsiMyXVOt7kR3t_g%3d%3d](#). DCSA will implement specific measures for covered JVs to ensure accountability and security compliance of covered JVs while performing on classified contracts.

4.3.3 Tribal Entity

An entity can be organized and existing under the law of an American Indian or Alaskan Native tribal entity under whose laws the entity is charter was formally acknowledged by the Assistant Secretary-Indian Affairs, of the U.S. Department of the Interior. When an entity is organized and continues to exist under the tribal statute or code, or other resolution authorized by a tribal legislative body, the facility should provide a charter, certificate of organization, or other applicable tribal documents and statute or code provisions governing the formation and continuation of the entity. [32 CFR 117.9(c)(2)(ii), [https://www.ecfr.gov/current/title-32/part-117#p-117.9\(c\)\(2\)\(ii\)](https://www.ecfr.gov/current/title-32/part-117#p-117.9(c)(2)(ii))]

4.4 Upgrades

The FCL upgrade process is largely the same with some key differences. The facility should have an established NISS account, as well as primary and alternate DISS account holders. The facility will submit an FCL package to the assigned ISR via NISS or successor system, and annotate any changes. Facilities undergoing an FCL upgrade will remain assigned to the local field office and ISR. The FCL packages will be reviewed by the ISR and then forward the FCL package to headquarters for review of risk or FOCI concerns.

Verify the SF-328, KMP list, and business documents are current and updated as necessary. One key difference in the FCL process for an upgrade is the facility is responsible for initiating any necessary upgrade PCL investigation requests for the required KMP. The upgrade PCL investigation requests should be initiated once the FSO has submitted the FCL package in NISS.

Please see the [associated business structure section](#) or slick sheet for additional information relating to required information, documentation, and KMP.

4.5 Additional Guidance on FCL Package Documentation

As a general note for all business types, organizations must register their business with a physical address. The physical address (not a P.O. Box or virtual office) is the actual address where the organization is doing business (maybe different than the state of incorporation/organization). This is the address DCSA uses for the FCL and is considered the home office/headquarters location. The CAGE code registration must also match this address. The documents listed below are specific to the in-process facility.



Documents/Forms	Additional Information
Business License	Dependent on the state and/or county in which the contractor operates
DD Form 441	- Agreement between your organization and the United States Government that details the security responsibilities of both the cleared organization and the USG - Execute one original DD Form 441 for DCSA and contractor retention - DD 441 must be signed by an employee or representative of the company who has authority to execute agreements with the USG on behalf of the company, such as the SMO DD Form 441 https://www.esd.whs.mil/Portals/54/Documents/DD/forms/dd/dd0441.pdf DD Form 441 Completion Sample
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, SF-328 DD Form 441-1 https://www.esd.whs.mil/Portals/54/Documents/DD/forms/dd/dd0441-1.pdf
Exclusion Resolution - Highest Cleared Entity Noting Excluded Entity's Exclusion	Executed by the in-process facility, acknowledging the exclusion resolution of the excluded tiered parent(s)
Exclusion Resolution of Corporate Organization	Executed by ultimate excluded U.S. parent, to include all excluded tiered entities (if applicable)
Exclusion Resolution for LLC Member (Organization)	Executed by LLC member(s), if organization
Exclusion Resolution for Certain Directors, Officers, and LLC Member (if Person)	- The company must submit exclusion resolution for KMP not required to be cleared in connection with the FCL - KMP that are not required to be cleared in connection with the FCL, but WILL require access to classified information in performance of the classified contract; please have the SMO provide a letter on company letterhead, stating that (KMP NAME) can be effectively and formally excluded from adversely effecting policies and procedures of the facility and that (KMP NAME) would require PCL eligibility in order to access classified information in the course of assigned duties and provide support on the classified contract
Fictitious Name Certificate (if applicable)	Must be provided if the company operates under a fictitious name, most commonly a DBA – doing business as
Formation Documentation	DCSA requires documentation demonstrating the contractor is organized and existing under the laws of the United States, one of the fifty States, the District of Columbia, or an organized U.S. territory (Guam, Commonwealth of the Northern Marianas Islands, Commonwealth of Puerto Rico, and the U.S. Virgin Islands)
Governance Documentation	DCSA requires documentation that details full control, and management of the company.



DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Legal Organizational Chart	▪ This shall reflect all U.S. and foreign parent companies, subsidiaries, branch/division offices, sister companies, and other affiliates. The Legal Organization Chart shall identify the associations between the cleared facilities and the tiered parents, including the percentages of ownership, percentages of control, FCL status, CAGE codes, citizenship/domicile and other helpful information explaining the relationship among the companies in the chain of ownership. ▪ See Appendix C
Meeting Minutes	▪ Provide the most recent Annual Meeting Minutes and any Meeting Minutes to reflect changes to a company's address, name, KMP, etc. which may be different than the operating agreement/by-laws etc. Please include brief description to identify the significance for each of the uploaded minutes. ▪ May be known at the facility by a different name, such as Memorandum for Record (MRF), Board Resolution, or other name(s).
Ownership Documentation	▪ DCSA requires documentation to validate the ownership and control of the company (i.e., Stock Ledger, Capitalization Table, Membership Interest List, Units Ledger).
Proof of Citizenship (if applicable)	▪ KMP requiring a PCL must provide citizenship verification in the form of a U.S. Passport, birth certificate, or Certificate of Naturalization.
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. ▪ Blank SF-328 https://www.dcsa.mil/Portals/128/Documents/CTP/FOCI/SF%20328%20(May%202025).pdf
Parent Facility/Facilities (if applicable)	▪ DCSA must account for full ownership/control throughout the entire business structure. ▪ Parent entities may need to submit business documents to provide DCSA ownership/control information. ▪ See specific business structure for a list of required documents outlining ownership and control for your parent facility.



5.0 Excluded Parent Process

As a part of the FCL process, DCSA must understand the complete, ultimate beneficial ownership of the facility, which may include parent facility(ies). A [parent](https://www.ecfr.gov/current/title-32/part-117#p-117.3(b)(Parent)) [https://www.ecfr.gov/current/title-32/part-117#p-117.3\(b\)\(Parent\)](https://www.ecfr.gov/current/title-32/part-117#p-117.3(b)(Parent)) facility is defined as a company owning greater than fifty percent of another company's voting securities. During the Review and Triage stage of the FCL lifecycle, DCSA will determine if a parent facility is required to obtain an FCL or if it can be excluded from access to classified information. If it is determined that a parent facility exercises the ability to control and/or manage the sponsored facility, to the extent that an exclusion resolution cannot be accepted, the parent facility must be processed for an FCL (commonly identified in the sponsored facility's governance documentation). If a parent facility cannot be excluded, it will be placed in process and cleared concurrently with the company that was awarded the contract.

For an Ultimate Excluded Parent (UXP), comprehensive business documentation is required as outlined in [section 4.2](#). This includes, but is not limited to, formation and governance documents, ownership information, and a KMP list detailing full legal name, titles, and citizenship. The UXP must also execute a consolidated SF-328 and a consolidated exclusion resolution that includes all intermediate XPs, as applicable and signed by the facility's SMO, Chairperson of Board, General Counsel, or other individuals with binding authorities.

Intermediate Excluded Parents (XPs) should provide documentation that identifies the full ownership structure, the state or country of organization, and a KMP list detailing full legal names, titles, and citizenship. All intermediate XPs should be included on the UXP's consolidated SF-328 and the corresponding exclusion resolutions. Further documentation may be requested by DCSA depending on the specific situation.



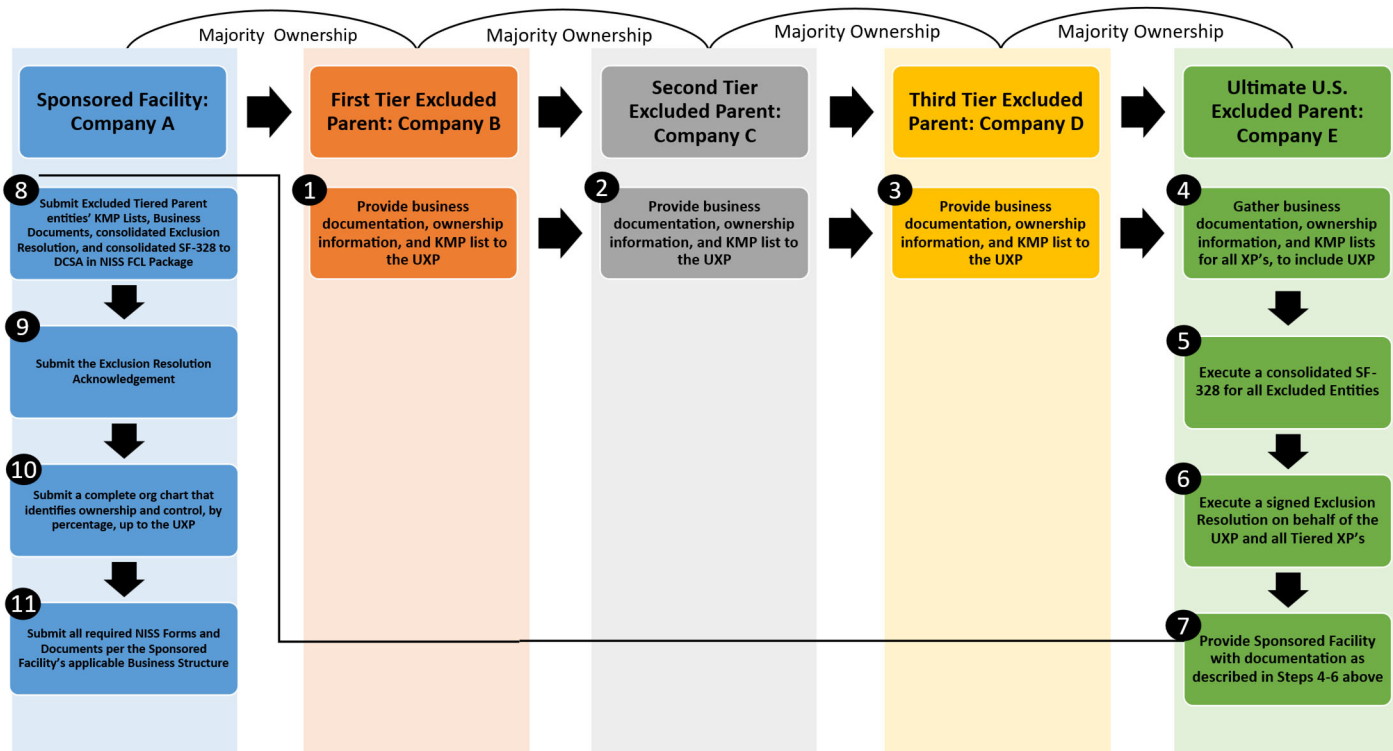
5.1 Sponsored Facility and Excluded Parent Definitions and Responsibilities

Facility	Definition	Responsibility
Sponsored/In-Process Facility (Highest Cleared Facility)	▪ The sponsored facility who is being processed for an FCL and/or the highest cleared facility in the corporate structure. • <i>In most cases, the sponsored facility will be the highest cleared facility in the corporate structure.</i>	▪ Submit XP's KMP Lists, business documentation, consolidated exclusion resolution, and consolidated SF-328 to DCSA via the NISS FCL Package • <i>Please label files specific to each respective facility and include a description of contents.</i> ▪ Submit the appropriate Exclusion Resolution Acknowledgement - (See Appendices I.1-I.4). ▪ Submit a complete organizational chart, identifying ownership and control, by percentage, up to the Ultimate Parent. ▪ Submit all required FCL Package documentation per its Business Structure.
Intermediate Excluded Parent Facility	▪ An intermediate parent facility is a company that owns a subsidiary but is itself also a subsidiary of another company. The intermediate parent facility is NOT the ultimate controlling company.	▪ Each intermediate XP must provide (to the Ultimate Parent) business documentation per their business structure, to include (but not limited to), formation documentation, governance documentation, ownership information, and KMP list (include full name and citizenship). The required business documentation is outlined in section 4.2 Business Structure Required Documents.
Ultimate U.S. Excluded Parent ▪ *ONLY provide business records, exclusions, KMP list, consolidated SF-328 from the Ultimate U.S. parent. This is NOT required for Ultimate Parents who are foreign.	▪ The ultimate parent is the top-most company in a corporate hierarchy. This entity owns or controls ALL other companies within the corporate structure, directly or indirectly, and is NOT controlled by another entity.	▪ The Ultimate U.S. XP must also provide its business documentation, per their business structure and a KMP list (include full name and citizenship). ▪ Provide Sponsored Facility with an organized compilation of intermediate XP business records and KMP list(s). ▪ Provide Sponsored Facility a consolidated SF-328 that includes information for all intermediate XPs. ▪ Provide Sponsored Facility with a signed Exclusion Resolution on behalf of the UXP and each intermediate XP. (See Appendices I.1-I.4)



5.2 Excluded Parent Workflow Example

The process flow below outlines the required documents the sponsored facility must provide to DCSA on behalf of any intermediate excluded parent (XP) and the ultimate excluded parent (UXP). In this process neither the ultimate excluded facility UXP) nor any of the intermediate tiered XP facilities hold an FCL.





6.0 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. Also, accounts and systems recommended for usage depending upon need.

Accounts	Reason for Account	Description
Commercial and Government Entity (CAGE) Code <i>Recommended</i>	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 facility 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. DLA CAGE LINK https://cage.dla.mil/Home/UsageAgree SAM LINK https://www.sam.gov/
Defense Information System for Security (DISS) <i>Required</i>	System to serve as the record to perform comprehensive personnel security, suitability, and credential eligibility management <i>Account MUST be established within 30 days of the FCL being issued</i>	DISS provides secure communication between Adjudicators, Security Officers, and Component Adjudicators in support of eligibility and access management. All PCL eligibility and access records for KMP and those requiring access to classified information must be kept up to date in DISS. Because a person cannot view or act on their own personnel record, cleared companies must have at least two (2) DISS account holders to comply with 32 CFR Part 117. Full DISS Account Request procedures are available on the DISS website. DISS LINK https://www.dcsa.mil/is/diss/
National Background Investigation Services (NBIS) Electronic Application (eAPP) <i>Required</i>	Submit KMP information through this system as part of the PCL process	eAPP, allows the user to electronically enter, update and transmit their personal investigative data over a secure internet connection to a requesting agency. EAPP LINK https://www.dcsa.mil/Systems-Applications/National-Background-Investigation-Services-NBIS/NBIS-eApp-NBIS-Agency/
National Industrial Security System (NISS) <i>Required</i>	System of record for facility clearances	NISS is the system of record for submitting and processing initial and upgrade FCL packages and change condition packages. NISS LINK https://www.dcsa.mil/is/niss/ <i>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</i> NCAISS LINK https://ncaiss-ps3.dss.mil/dss-cac-login/cert/login



DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Secure Web Fingerprint Transmission (SWFT) <i>Recommended</i>	Submit KMP fingerprints through SWFT or third-party vendor to complete KMP PCL process <i>Account created after the facility is issued its FCL</i>	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) <i>For SWFT access requests, please refer the SWFT resources https://www.dcsa.mil/Systems-Applications/Secure-Web-Fingerprint-Transmission-SWFT/SWFT-Resources/ section on the DCSA website</i> SWFT LINK https://www.dcsa.mil/is/swft/
DoD SAFE <i>As necessary</i>	Approved for CUI/PII/PHI file exchange.	DoD SAFE allows for file exchange between facility's and DCSA when CUI, PII, or PHI information is involved. Web-based file transfer service that provides authenticated DoD Common Access Card (CAC) users (authenticated users) and guests (unauthenticated users) the capability to securely send and receive large files, including files that are too large to be transmitted via email. DoD SAFE LINK https://safe.apps.mil/
Security Training, Education, and Professionalization Portal (STEPP) <i>Recommended</i>	Provides training and educational courses for security professionals	Program maintaining the list of training and educational courses that DCSA offers to security professionals. The courses are intended for use by DoD and other USG personnel and contractors within the NISP STEPP LINK https://www.cdse.edu/
National Industrial Security Program (NISP) Enterprise Mission Assurance Support Service (eMASS) <i>As necessary</i>	Provides standardized Risk Management Framework (RMF) process support and storage for cyber security artifacts for assessment by cleared industry and DCSA security professionals <i>Account Requirements:</i> • Complete DISA eMASS training https://www.cdse.edu/Training/eLearning/DISA-100/ on STEPP (DISA100.06) • Complete DoD Cyber Awareness Challenge (STEPP or DoD Cyber Exchange https://public.cyber.mil/training/cyber-awareness-challenge/) • Submit DD 2875 SAAR https://www.esd.whs.mil/portals/54/documents/dd/forms/dd/dd2875.pdf	eMASS is an application that automates the DCSA Assessment and Authorization Process Manual (DAAPM) tasks supporting the RMF used by the DoD, other USG Agencies, and the NISP industry participants NISP eMASS Link https://nisp.emass.apps.mil/



7.0 Tools and Training

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.

Tools and Resources	Link
Center for Development of Security Excellence (CDSE) Toolkits	https://www.cdse.edu/toolkits/index.html
Facility Security Officer (FSO) Toolkit	https://www.cdse.edu/Training/Toolkits/FSO-Toolkit/
Insider Threat Program Senior Official (ITPSO) Toolkit	https://www.cdse.edu/Training/Toolkits/Insider-Threat-Toolkit/
National Industrial Security Program (NISP) Tools and Resources	https://www.dcsa.mil/Industrial-Security/National-Industrial-Security-Program-Oversight/NISP-Tools-Resources/
DCSA Risk Management Framework (RMF) Toolkit	https://www.cdse.edu/Training/Toolkits/Information-System-Security-Manager-Toolkit/
RMF Knowledge Service <i>(when applicable)</i>	https://rmfks.osd.mil/login.htm
Security Shorts and Security Training Videos	https://www.cdse.edu/Training/Security-Shorts/ https://www.cdse.edu/Training/Security-Training-Videos/

7.1 FSO Training

A list of the required FSO Training is available in the FSO Toolkit. FSOs of facilities that require safeguarding must complete the FSO Program Management for Possessing Facilities. FSOs of companies that do not require safeguarding should complete the FSO Orientation for Non-Possessing Facilities. Both courses are offered on the Security Training, Education and Professionalization Portal (**STEPP** <https://www.cdse.edu/>). The appointed FSO will need to take the applicable 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 facility's requirements under the NISP. The FSO must complete the required training within 6 months of appointment ([32 CFR 117.12\[d\]](https://www.ecfr.gov/current/title-32/part-117#p-117.12(d)) [https://www.ecfr.gov/current/title-32/part-117#p-117.12\(d\)](https://www.ecfr.gov/current/title-32/part-117#p-117.12(d))).

7.2 Insider Threat Program Training

The SMO is required to appoint an Insider Threat Program Senior Official (ITPSO). This person will be considered a KMP along with the FSO, SMO, and other KMP. The ITPSO can be the same or different individual as SMO, and/or the FSO. Corporate families may nominate a corporate ITPSO.

The ITPSO **MUST** take one of the trainings listed below. Newly appointed insider threat program personnel can satisfy minimum training requirements by either completing the Center for Development of Security Excellence (CDSE) "Insider Threat Program for Industry Curriculum,



INT333.CU” or by completing a contractor-developed training program. Importantly, insider threat program personnel appointed prior to July 1, 2025, who have already completed training are not required to complete the new curriculum:

- [Insider Threat for Industry Curriculum](https://securitytraining.dcsa.mil/course/search.php?areaid=core_course-course&q=ITPSO)
https://securitytraining.dcsa.mil/course/search.php?areaid=core_course-course&q=ITPSO
- Create their own training that covers the topics outlined in [32 CFR 117.12\(g\)\(1\)](https://www.ecfr.gov/current/title-32/part-117#p-117.12(g)(1))
[https://www.ecfr.gov/current/title-32/part-117#p-117.12\(g\)\(1\)](https://www.ecfr.gov/current/title-32/part-117#p-117.12(g)(1)). Requires review by DCSA IS HQ, email: dcsa.quantico.dcsa.mbx.isd-nmp-div@mail.mil. Allow 30 days for review.
- Combine contractor-developed training with existing DCSA designated courses to cover all the topics outlined in [32 CFR 117.12\(g\)\(1\)](https://www.ecfr.gov/current/title-32/part-117#p-117.12(g)(1)) [https://www.ecfr.gov/current/title-32/part-117#p-117.12\(g\)\(1\)](https://www.ecfr.gov/current/title-32/part-117#p-117.12(g)(1)).

The ITPSO **MUST** also certify that a written Insider Threat Program is in place. Your ISR will discuss it further during the Orientation Meeting. Additional information, including a plan template, job aid, and toolkit is available at the [Industry Insider Threat and Resources](https://www.cdse.edu/Training/Toolkits/Insider-Threat-Toolkit/)
<https://www.cdse.edu/Training/Toolkits/Insider-Threat-Toolkit/> on DCSA website.



Appendix A: Common KMP Authorities by Position

This does not include the authorities of the FSO ([32 CFR 117.7\(b\)\(3\)](https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117#p-117.7(b)(3))) or the ITPSO ([32 CFR 117.7\(b\)\(4\)](https://www.ecfr.gov/current/title-32/part-117#p-117.7(b)(4))) [https://www.ecfr.gov/current/title-32/part-117#p-117.7\(b\)\(4\)](https://www.ecfr.gov/current/title-32/part-117#p-117.7(b)(4))). Additionally, this does not include all possible roles, positions or titles which might result in an essential KMP.

KMP Role	Authorities of the Position
Board of Directors	- Protects shareholders' assets and ensures 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 - Oversees share repurchase programs, recommend stock splits, etc. - Recommend or discourages mergers and acquisitions
Chairman of the Board	- Trusted with the responsibility of chairing a board - Governs the board according to the by-laws of the organization. The chairman must attend the board meetings and committees regularly. - Committed to board duties and has vast knowledge of the organization - Evaluates annual performance of the organization - Chairman rarely involves themselves in the company's day-to-day operations; instead concentrates on the bigger picture and various strategies to increase the company's bottom line - Institutes and enforces company policies and guidelines - Recruits, interviews, and hires the CEO - Votes on key issues surrounding the company; when the board is at a standstill on an issue, the chair typically makes the final decision
Chief Executive Officer (CEO)	- Highest ranking executive manager in a corporation or organization's governance documentation - Responsible for the overall success/management of the organization - Ultimate authority to make final decisions for an organization - Responsible for creating, planning, implementing, and integrating the strategic direction/vision of an organization - Reports to the Board of Directors and serves at the discretion of the Board of Directors
Chief Operating Officer (COO)	- Responsible for the daily operations - Provides communication, leadership, and guides management as necessary to ensure that facility 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 them 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 practices to maximize the financial integrity of the Company - Ensures appropriate and satisfactory systems are in place for monitoring - Company performance against planned and budgeted expectations
General Partner (GP)	- Full management control and accepts full personal responsibility for partnership's liabilities, as specified by state law where the partnership was formed and the partnership agreement - Right to manage the business, conduct transactions on behalf of the business, and are liable for company debts - Commonly is active in the day-to-day operations of the business - May be an individual or facility



KMP Role	Authorities of the Position
Limited Partner (LP)	- Generally, it 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
Manager	- For a manager-managed 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 the LLC is formed - Elected by the members. The member(s) may be elected to be the manager. - Decision authority on key policies, transactions, and establishment of guidelines for how the LLC will operate - Can appoint officers (if supported in the OA) to serve at the pleasure of the manager or board of managers.
Member	- For a member-managed LLC, like a stockholder in a corporation. The member is responsible for the formation of the LLC and have an owning interest in the LLC, as designated in the Operating Agreement, and/or State Law when there is no Operating Agreement - Member-managed LLC, the control is retained by the member
President	- May be the highest-ranking executive manager in a corporation or organization's governance documentation if there is no CEO or equivalent. - 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 - Oversee the organization in accordance with the direction established in the strategic plans
Shareholder or stockholder	- Can be a person or an entity - 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
Vice President (VP)	- Second in command of an organization and has specific responsibilities depending on the needs of the organization, as directed in 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 - Vice President acts in the absence of the President



DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Appendix B: Sample DD-441, SF-328, and SF-328 Signature Pages

B.1 DD Form 441 Completion Sample

DoD 5220-22-M

DEPARTMENT OF DEFENSE SECURITY AGREEMENT		OMB No. 0704-0194 OMB approval expires 20201031	
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, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Project Director (0704-0194), Washington, DC 20503. 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.			
This DEPARTMENT OF DEFENSE SECURITY AGREEMENT (hereinafter called the Agreement), entered into this day of 20 by and between THE UNITED STATES OF AMERICA through the Defense Counterintelligence and Security Agency acting for the Department of Defense and other governmental User Agencies (hereinafter called the Government), and (hereinafter called the Contractor), which is: DO NOT FILL IN THE DATE ENTER COMPANY'S LEGAL NAME (1) A ENTER COMPANY'S BUSINESS STRUCTURE 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 future purchase from the Contractor, which are required and necessary; United States; or may invite to proposed contracts for the purchase are required and necessary to the States; and WHEREAS, it is essential that taken by the Contractor prior to a to classified information; and WHEREAS, the parties desire precautions and specific safeguard and the Government in order to protect the United States through the protection of classified information, sabotage the security of the United States; NOW, THEREFORE, in consideration of the mutual promises herein contained, the parties agree to the following: Section I - SECURITY CONTROL (A) The Contractor agrees to place security controls within the organization requirements of the "National Operating Manual," DoD 5220 Manual) attached hereto and in subject, however, (i) to any revision demands of national security as in notice of which shall be furnished mutual agreements entered into in the Manual to the Contractor procedures thereunder.			
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 of the day and year written above: THE UNITED STATES OF AMERICA By LEAVE BLANK (Signature of Authorized Government Representative) LEAVE BLANK (Typed Name of Authorized Government Representative) LEAVE BLANK (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'S 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(S) (Title of Authorized Contractor Representative) COMPANY'S STREET ADDRESS (Contractor Address) COMPANY'S CITY, STATE, ZIP (Contractor Address) SMO'S TITLE(S) By executing this form, the Contractor Representative certifies that he or she is the of the business entity identified above, and has the authority to bind the business entity to the terms of this agreement.	
DD FORM 441, FEB 2020		DD FORM 441 (BACK), FEB 2020	

PREVIOUS EDITION IS OBSOLETE.

RESET



B.2 SF-328 Certification

Certificate Pertaining to Foreign Interests (SF-328), is a 9-question form in which a facility identifies foreign ownership, control, or influence (FOCI) in its organization. Answer yes or no, as applicable to your facility, any “yes” answers require additional details. Please see the SF-328 Completion Instructions for the information required for each affirmative response. The blank SF-328 can be found here:

[https://www.dcsa.mil/Portals/128/Documents/CTP/FOCI/SF%20328%20\(May%202025\).pdf](https://www.dcsa.mil/Portals/128/Documents/CTP/FOCI/SF%20328%20(May%202025).pdf)

Consolidated SF-328s

- Highest cleared U.S. entity: The highest cleared entity in the corporate chain is required to submit a consolidated SF-328 including information from itself and all other cleared subsidiaries, branches, or divisions beneath it. This entity is also responsible for ensuring timely reporting of changed conditions impacting the corporate chain.
- Highest uncleared U.S. parent: Facilities with uncleared U.S. parent facilities in their ownership and control structure will be required to submit a parent SF-328. This SF-328 will include the consolidated information for all uncleared U.S. entities in the cleared facility’s corporate chain.

	YES	NO
1. Does any foreign person(s), directly or indirectly, own, beneficially own, or subscribe to 5 percent or more of the outstanding shares of any class of stock, participation interest, units, or total capital commitment for your organization?	☐	☐
2. Does your organization directly or indirectly through your subsidiaries and/or affiliates, own 10 percent or more of any foreign interest(s)?	☐	☐
3. Do any foreign persons serve as a member of your organization's governing body, or hold a management position?	☐	☐
4. Does any foreign person(s) have binding authority or the power, direct or indirect, whether or not exercised, to control the election, appointment, or tenure of members of your organization's governing body or other management positions of your organization, or have the power to control or direct any decisions or activities of your organization?	☐	☐
5. Does your organization have any contracts, agreements, understandings, grants, side letters, or arrangements with a foreign person(s)?	☐	☐
6. Does your organization, whether as borrower, surety, guarantor, or other, have any indebtedness, liabilities, or obligations to a foreign person(s)?	☐	☐
7. During your organization's last fiscal year, did it derive:		
a. 5 percent or more of its total revenue, net income, tuition, gifts, or endowments from any single foreign person?	☐	☐
b. In the aggregate, 15 percent or more of its revenue, net income, gifts, tuition, or endowments from foreign persons?	☐	☐
8. Does any individual(s) holding management positions within your organization hold positions with, or serve as consultants or representatives for any foreign person(s)?	☐	☐
9. Is there any information, not provided in response to previous questions on this form, indicating that a foreign person(s) could control or influence the operations or management of your organization in a manner that allows unauthorized access to U.S. government information or that may adversely affect performance of U.S. government contracts?	☐	☐

Instructions for Completing the Standard Form 328 and Supporting Documents are included and begin after the signature block. Please review the instructions in full and answer all subsequent questions for all affirmative answers.



DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Instructions for Completing the Standard Form 328, "Certificate Pertaining To Foreign Interests" and Submitting Supporting Documents

This document explains how to appropriately respond to Standard Form 328 (SF-328) questions and supporting document requirements for each response. The instructions below are not exhaustive and may require the organization to determine what similar or equivalent information will meet the spirit and intent of the question. SF-328s not addressing the mandatory items set forth in this document will be treated as incomplete and could lengthen processing times.

Material Change: Updates to the SF-328 are required in accordance with applicable Industrial Security Letters or U.S. government requirements. Organizations reporting a material change to the SF-328 must include a complete explanation of how the organization's foreign ownership, control or influence has changed since its last submission.

NOTE: All responses referencing supporting documentation must include the name and date of the document, and specific page number, section, or paragraph supporting each response.

NOTE regarding definitions: Unless otherwise stated, the definitions of terms in this form are the same as those found in 32 CFR 117.3

B.3 SF-328 Certification (Signature Block) Example

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. I CERTIFY that I have been duly appointed to the position title below of the business entity and have the authority to bind the business entity to the terms of this form.	
WITNESS:	
Digital or ink signature of witness	Date certified, should match the witness signature date
	(Date Certified)
Date of witness signature	Digital or ink signature of the Authorized Contractor Representative (typically the SMO)
(Date)	By
	Typed name of the Authorized Contractor Representative
	(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.	Title(s) of Authorized Contractor Representative
	(Title of Authorized Contractor Representative)
	Full Legal Name and Address of Facility
	(Address)

Page of

CUI (when filled in)

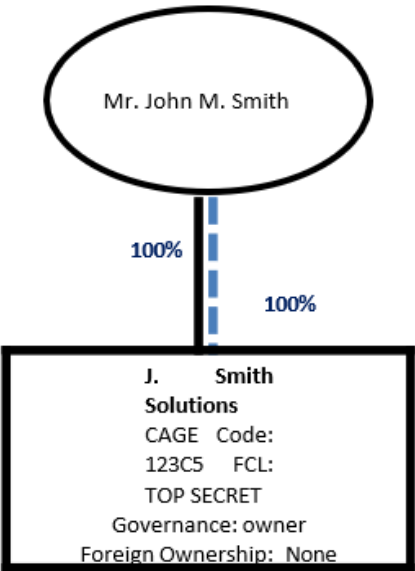
STANDARD FORM 328 (REV. 5/2025)

PREVIOUS EDITION IS OBSOLETE.



Appendix C: Sample Organizational Charts

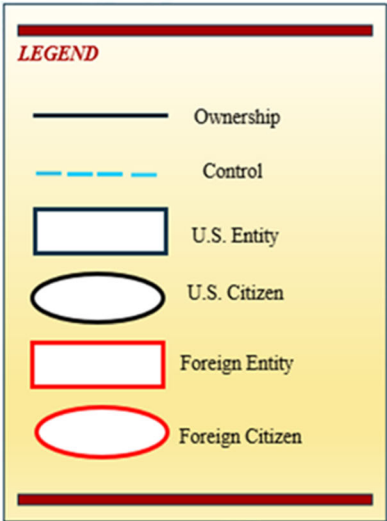
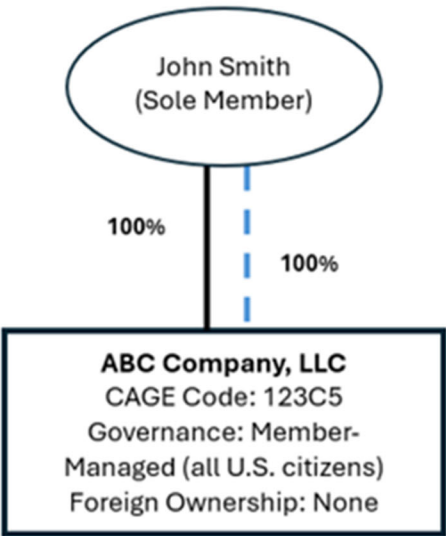
C.1 Sole Proprietorship





C.2 LLC (Member-Managed)

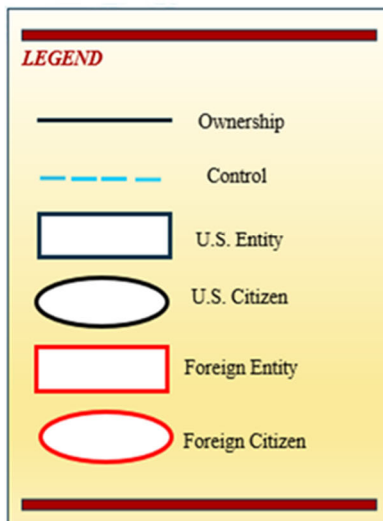
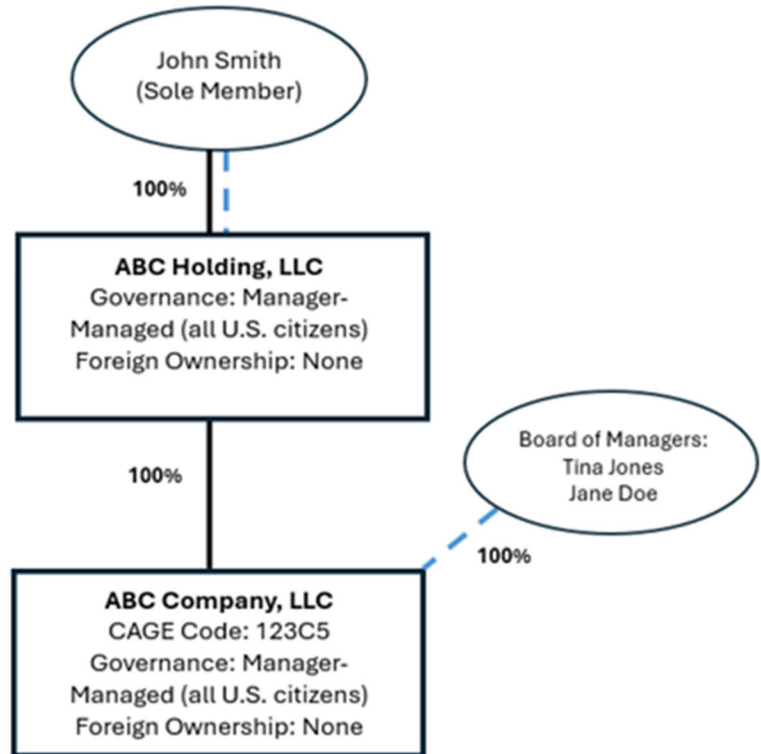
ORGANIZATIONAL CHART (Sample: Member-Managed LLC)





C.3 LLC (Manager-Managed)

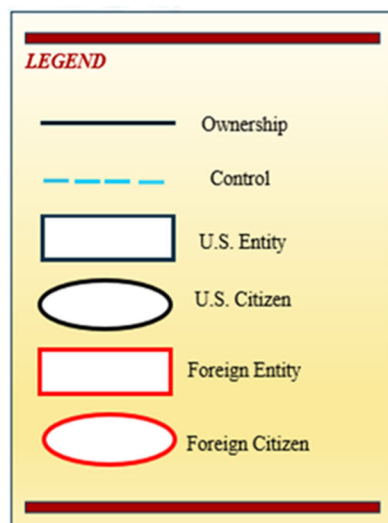
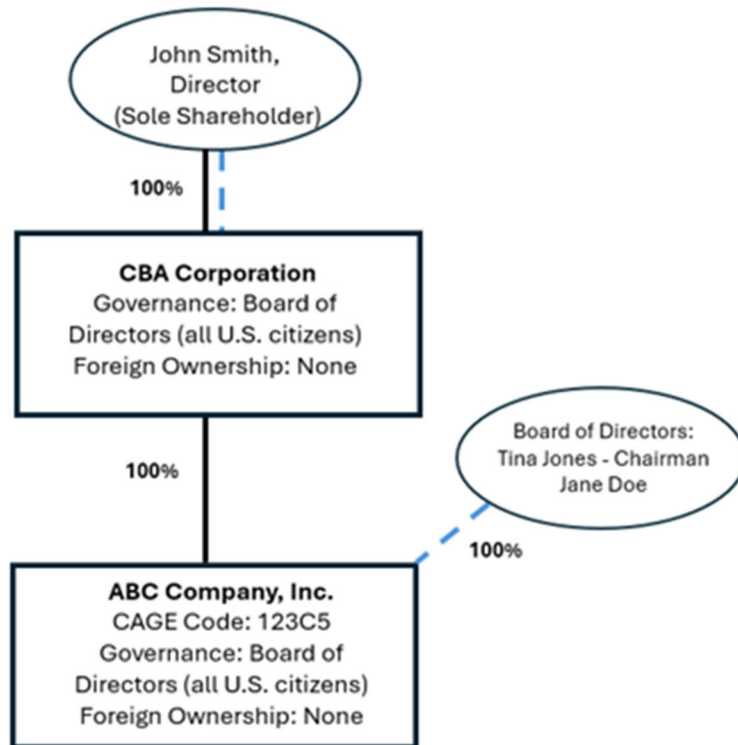
ORGANIZATIONAL CHART (Sample: Manager-Managed LLC)





C.4 Corporation

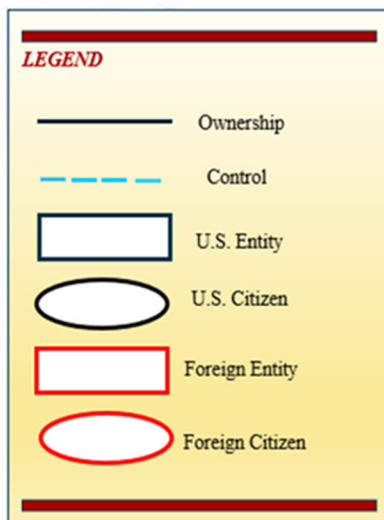
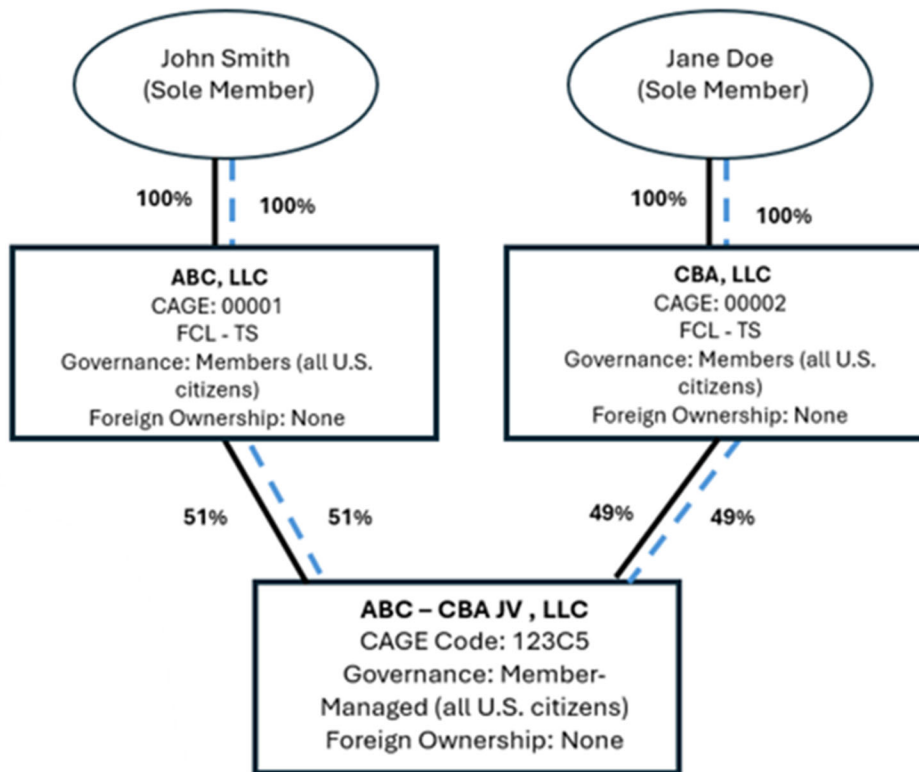
ORGANIZATIONAL CHART (Sample: Corporation)





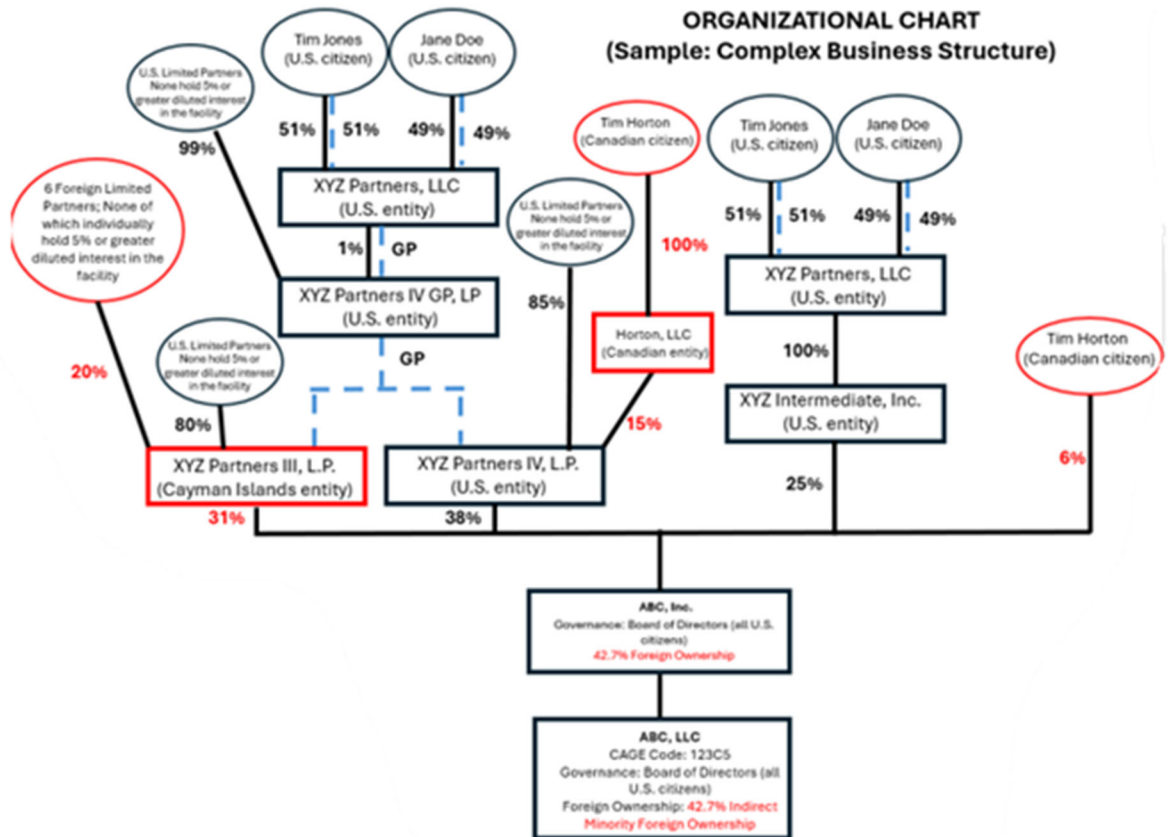
C.5 Joint Venture

ORGANIZATIONAL CHART (Sample: Joint Venture)





C.6 Complex Business Structure



LEGEND

- Ownership
- Control
- U.S. Entity
- U.S. Citizen
- Foreign Entity
- Foreign Citizen

Note: Identify any LPs with 5% or greater ownership (identify if U.S. or foreign)

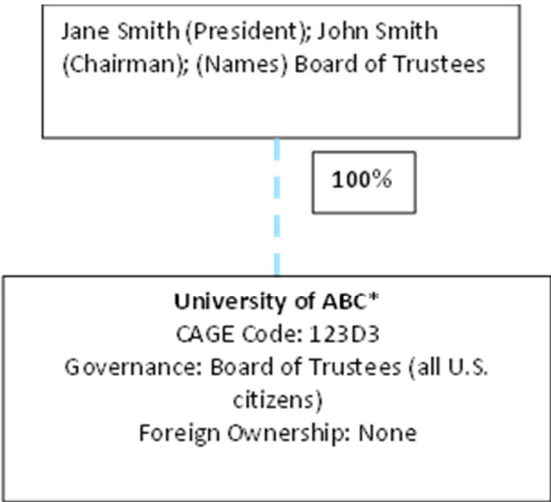
Note: Identify GPs (identify if U.S. or foreign)

Note: Identify the total percentage of individuals or entities with less than 5% ownership (in aggregate).

Note: Identify if any foreign country's ownership aggregates to 5% or greater



C.7 University Structure



LEGEND

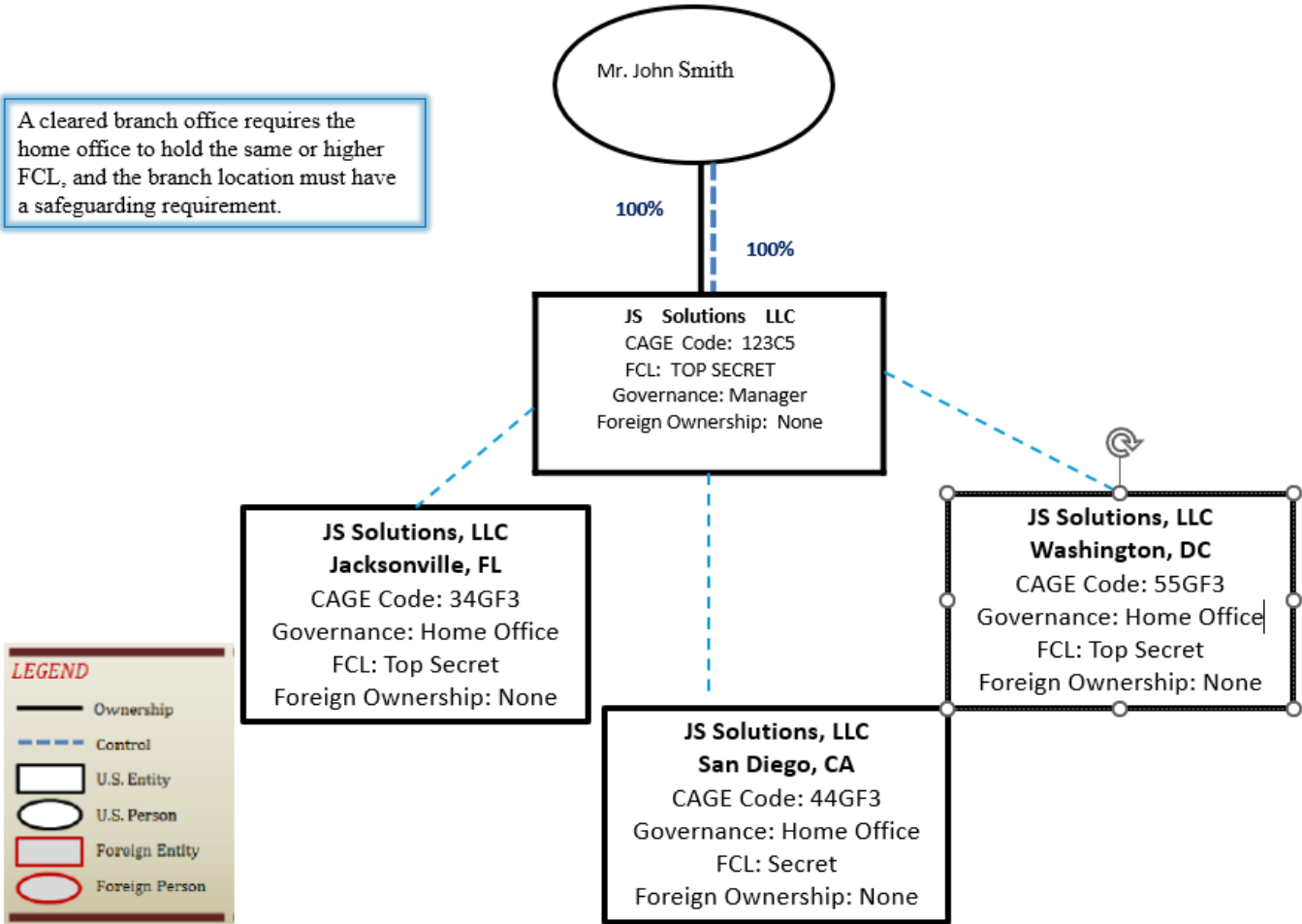
	Ownership
	Control
	U.S. Entity
	U.S. Citizen
	Foreign Entity
	Foreign Citizen

**Organized as a 501(c)(3) nonprofit organization that is not beneficially owned by one individual or company: chartered by the government of the State of ABC.*



C.8 Branch Offices

A cleared branch office requires the home office to hold the same or higher FCL, and the branch location must have a safeguarding requirement.





Appendix D: FCL Package Common Errors List

This is not an exhaustive list of all errors. This list is intended to assist facilities in avoiding common reasons for rejection of the FCL package.

Basic Information and Documentation

1. On the basic information tab in NISS, please confirm the business structure selected is correct
2. On the basic information tab in NISS, include all prior legal facility names and prior legal addresses
3. Confirm all required documentation is provided for the appropriate [business structure](#)
4. Do not use zip files and do not upload documents altogether under one file - each specific document should be uploaded under corresponding document type/tab, within the FCL package
5. Confirm the principal place of business listed in System for Award Management (SAM), the Secretary of State website(s), and ensure provided business documentation matches, or the discrepancy is addressed
6. Confirm the facility is registered to conduct business within the state it is/will be operating in, even if organized in a different state (i.e., principal address located in Virginia, although organized in Delaware)
7. Provide documentation reflecting business structure conversion, if applicable (i.e., LLC to an Inc.)
8. Ensure all authorized stock shares are accounted for, including un-issued shares, ESOPs, etc.
9. The [Legal Organizational Chart](#) shall reflect all U.S. and foreign parent companies, subsidiaries, branch/division offices, sister companies, and other affiliates. It shall identify the associations between the cleared facilities and the tiered parents, including the percentages of ownership, percentages of control, FCL status, CAGE codes and other helpful information explaining the relationship among the companies in the chain of ownership

SF-328 and DD Form 441

1. As referenced in the instructions, please provide detailed explanation(s) to affirmative answers on the [SF-328](#)
2. Ensure the [SF-328](#) & [DD-441](#) are signed by the [SMO](#), witnessed, and dated the same day
3. On the [SF-328](#) & [DD-441](#), ensure the titles for Authorized Contractor Representative and the certifying official match
4. On the [DD-441](#), ensure the date field is blank on the first page
5. On the [DD-441](#) signature block, ensure the facility name is on the line titled “typed name of contractor entering agreement”
6. Do not leave the very last line blank on either the [SF-328](#), or the [DD-441](#)

KMP Information and KMP List

1. Confirm the Personally Identifiable Information (PII) (spelling of names, Social Security Number, date of birth, etc.) is correct
2. Provide the FSO appointment date on the KMP list in NISS
3. Do not identify the Assistant/Alternate Facility Security Officer (AFSO) on the KMP List. The AFSO is not a KMP nor is the position required to be cleared in connection with the FCL
4. Identify everyone only once and include all designated titles associated with that individual
5. Confirm the designated titles are supported by the governance documents (Operating Agreement/By-laws etc.). Provide documentation reflecting the election/appointment of the Officers/Board Members, etc.



6. All [required positions](#) as defined in the business documents **MUST** be on the KMP list. If the required position is currently not filled, list as VACANT on the KMP list
 - a. Example: First Name: VACANT; Last Name: VACANT; Essential KMP (Required to be cleared in connection with FCL): NO; Title: INSERT VACANT POSITION TITLE
7. Confirm [SMO](#) is identified on the KMP list. The SMO is not a position that can be appointed but is determined based on the facility's governance documents. NOTE: there are rare circumstances in which there may be more than one SMO (i.e., two individuals both have 50% ownership, and control of the facility).
8. Provide the exclusion resolution for any non-essential KMP also known as [excluded KMP](#). If a non-essential KMP requires access to classified information in support of the classified contract, please have the SMO provide a letter on company letterhead stating that (KMP NAME) can be effectively and formally excluded from adversely affecting policies and procedures of the facility and that (KMP NAME) will require PCL eligibility to access classified information in the course of assigned duties on the classified contract.
9. Upload [proof of citizenship](#) for those essential KMP that don't already possess a PCL.
10. Companies are not to be included on the KMP list.

Excluded Parent Information (if applicable)

1. Provide business records for each tiered parent based on their business structure as outlined in section [4.2 Business Structure-Specific KMP and Required Documentation](#).
2. Provide the documentation reflecting the election/appointment of the Officers/Board Members, etc.
3. Provide KMP list for each tiered parent to include individual name and citizenship.
4. The highest [excluded parent](#) facility shall execute a [consolidated SF-328](#) that includes information for all excluded entities.
5. The highest [excluded parent](#) facility should execute an exclusion resolution on behalf of its facility and all intermediate/tiered parents to be excluded.
6. The sponsored facility should execute an exclusion resolution acknowledging the excluded tiered entities' consolidated exclusion resolution.



Appendix E: FCL Package RFI Process

The FCL Package RFI (Request for Information) process described below is not exclusive as to possible reasons for discontinuation of the FCL process.

Overview:

Effective March 1, 2023, DCSA implemented a procedure for facility clearance (FCL) package submissions to reduce the cycle, or re-work, between government contracting activities (GCAs) or contractors and DCSA. This change is one of several initiatives DCSA undertook to streamline the FCL process, which will ensure the fullest degree of transparency practicable during the sponsorship and FCL package processes. DCSA encourages the full utilization of available resources from DCSA by sponsors or the sponsored contractors to ensure complete and accurate packages are submitted to facilitate DCSA's efficient and thorough evaluation of each case.

Applicability:

These updated procedures apply to the following package types submitted by GCAs/Contractors: Sponsorship, Initial FCL, and Upgrade FCL.

Procedures:

DCSA is implementing the procedures outlined below:

1. GCA or Contractor submits a package via NISS (or subsequent system of records used).
2. DCSA conducts the first review of the package for completeness and/or a legitimate requirement.
 - 2.1. Incomplete Package: DCSA returns the package to the original submitter via NISS (or subsequent system of records used) with details concerning the missing information or items to be corrected DCSA will provide resources (policy, forms, templates, etc.) that can be used to address the reasons for the return and point of contact (POC) information should question or concerns arise. DCSA will provide a suspense date for resubmission (see step 3).
 - 2.2. Complete Package: DCSA accepts the package and continues processing. GCAs or Contractors may check NISS or their case-specific POCs for status information. In addition, GCAs or Contractors may contact the Knowledge Center for basic status requests.
3. GCA or Contractor reviews the details provided by DCSA concerning the missing information or items requiring correction.
 - 3.1. Request Extension: In the rare case when an extension is needed, the GCA or Contractor will contact their DCSA POC via email no later than three business days prior to the suspense date to request an extension. Extension requests must contain the proposed suspense date requested and a justification supporting the extension request. DCSA will notify the submitter if the extension request is deemed acceptable or will provide an updated suspense.
 - 3.2. Resubmit: GCA or Contractor addresses missing or incorrect information within the



package. The package must contain an overview of what corrective actions were taken to address each of the details provided by DCSA. Once all items have been addressed, the GCA/Contractor resubmits the package.

4. DCSA conducts a review of the resubmitted package for completeness.

4.1. Incomplete Package: (DCSA request(s) not addressed): If the package still contains the same inaccurate or missing information, DCSA will take the following actions:

4.1.1. Initial FCL/Upgrade Package Actions: DCSA discontinues the FCL process resulting in the removal of the package and request from DCSA's queue. In such cases, the GCA or Contractor must submit a new FCL Package request (new sponsorship not required).

4.2. Complete Package: DCSA accepts or approves the package and continues processing. GCAs or Contractors may check NISS or their case-specific POCs for status information. In addition, GCAs or Contractors may contact the Knowledge Center for basic status requests.

5. Notification Process: To increase transparency within the process, DCSA will notify the affected parties when returning, rejecting, or discontinuing a package.

5.1. Sponsorship Packages: DCSA will notify the Sponsored Contractor of the Sponsorship Package being returned or rejected. DCSA will refer the Contractor to their Sponsor if additional details are required.

5.2. Initial FCL/Upgrade Packages: DCSA will notify the Sponsor of the incomplete FCL Package submission and subsequent FCL process discontinuation. DCSA will refer the Sponsor to the Sponsored Contractor if additional details are required.



Appendix F: FCL Discontinuation

The FCL Process can be discontinued for reasons which include but are not limited to:

- Failure to communicate with DCSA
- Failure to submit or return a RFI by the provided due dates
- Failure to submit a complete and accurate FCL process within an appropriate timeframe
- Failure to submit all necessary PCL investigation requests and/or fingerprints by the provided due dates
- Other reasons as deemed appropriate by DCSA Leadership

If the FCL process is discontinued, DCSA will complete the necessary action within NISS stopping the FCL process. The facility and sponsor will receive an email notification of the discontinuation and an explanation as to why. The facility will need to coordinate with the sponsor for resubmission of the FCL Sponsorship request. In some circumstances, typically those outside the control of the facility, DCSA will restart the FCL process workflow within NISS when requested by the facility or sponsorship allowing the process to continue.



Appendix G: PKI/ECA – access to NCAISS and NISS

For FSOs who are not being issued a Common Access Card, it is recommended to purchase a medium token assurance hardware-based certificate immediately following notification of contract award and the need for a facility clearance (FCL). It can take two or more weeks to obtain the PKI/ECA once all documentation is submitted, and starting the process as early as possible avoids delays in processing the FCL.

The DCSA National Industrial Security Program (NISP) Central Access Information Security System (NCAISS Portal, <https://ncaiss.dss.mil/>) is a web-based application that provides Public Key Infrastructure (PKI)-based authentication services to DCSA applications and information systems for authorized users. NCAISS access is required for access to the National Industrial Security System (NISS), the system of record for FCL processing and industrial security oversight. Through the NCAISS Portal, an authorized user can access their DCSA NCAISS Portal account via a single sign-on (SSO) capability using PKI certificates (either a Common Access Card or DoD-approved External Certification Authority (ECA) certificate). The NCAISS database accepts all DoD-Approved PKIs. Thus, NISS cannot be accessed until a PKI/ECA is obtained and an NCAISS account is created.

Third-Party Vendors

Approved ECA Vendors:

- [Widepoint https://eca.orc.com/](https://eca.orc.com/)
- [Identrust, INC. https://www.identrust.com/digital-certificates/dod-eca-programs](https://www.identrust.com/digital-certificates/dod-eca-programs)

Choose your preferred vendor and follow the external vendor's instructions to purchase your PKI

Final Purchase

Complete the necessary identity proofing to begin the purchase process. Then, when prompted select the **Medium Token Assurance hardware-based certificate** PKI option.

Once PKI has been purchased, you will receive instructions from your chosen vendor on how to obtain and set up your PKI and hardware.

Additional Resources

DoD PKI Help Desk disa.gsd.maops@mail.mil
(844) 347-2457 Option 1,3,4

- ECA PKI Support: [PKI/PKE Help https://public.cyber.mil/pki-pke/help/](https://public.cyber.mil/pki-pke/help/)
- ECA Website: [ECA Home https://public.cyber.mil/eca/](https://public.cyber.mil/eca/)
- PKI Interoperability Website: [PKI/PKE Home https://public.cyber.mil/pki-pke/interoperability/](https://public.cyber.mil/pki-pke/interoperability/)
- [DoD ECA X.509 Certificate Policy https://dl.dod.cyber.mil/wp-content/uploads/eca/pdf/unclass-eca_cp.pdf](https://dl.dod.cyber.mil/wp-content/uploads/eca/pdf/unclass-eca_cp.pdf)
- [Frequently Asked Questions https://www.cyber.mil/faqs](https://www.cyber.mil/faqs)

Additional information on NISS can be found at: <https://www.DCSA.mil/is/ncaiss/>. You can also find information on how to setup your NISS account by accessing the job aid titled, DCSA OCIO NISP NCAISS User Guide

https://www.dcsa.mil/Portals/128/Documents/IS/DCSA_NCAISS_PS3_NCAISS_User_Guide.pdf.



Appendix H: Common Acronyms

AA&E - Arms, Ammunition & Explosives
AOP - Affiliated Operations Plan
BR - Board Resolution
CA - Controlling Agency
CFIUS - Committee on Foreign Investment in the United States
CIA - Central Intelligence Agency
CMMC - Cybersecurity Maturity Model Certification
CNWDI - Critical Nuclear Weapon Design Information
COMSEC - Communications Security
COTS - Commercial-off-the-shelf
CSA - Cognizant Security Agency
CSO - Cognizant Security Office
CUI – Controlled Unclassified Information
DCSA - Defense Counterintelligence Security Agency
DDD - Due Diligence Division
DESP - Defense Enhanced Security Program
DHS - Department of Homeland Security
DISS - Defense Information System for Security
DoD - Department of Defense
DOE - Department of Energy
ECP - Electronic Communications Plan
EV - Entity Vetting Directorate
FCL - Facility clearance
FLP - Facilities Location Plan
FOCI - Foreign ownership, control, or influence
FSO - Facility Security Officer
GCA - Government Contracting Activity
ISD – Industrial Security Directorate
ISOO - Information Security Oversight Office
ISSP - Information System Security Professional
ITPSO - Insider Threat Program Senior Official
KMP - Key management personnel
LAA - Limited Access Authorization
MFO - Multiple Facility Organization
NAESOC - National Access Elsewhere Security Oversight Center
NATO - North Atlantic Treaty Organization
NID - National Interest Determination
NISP - National Industrial Security Program
NISS – National Industrial Security System
NRC - Nuclear Regulatory Commission
NTIB - National Technology and Industrial Base
OD - Outside Director
ODNI - Office of the Director of National Intelligence
PA - Proxy Agreement
PCL - Personnel security clearance



PH - Proxy Holder
PNT - Position, Navigation, and Timing
RD - Restricted Data
RF - Radiofrequency
RMD - Risk Management Division
SaaS - Software as a Service
SAP - Special Access Program
SCA - Security Control Agreement
SCI - Sensitive Compartmented Information
SMO - Senior Management Official
SSA - Special Security Agreement
TCP - Technology Control Plan
USD(I&S) - Undersecretary of Defense (Intelligence & Security)
VT - Voting Trust
XP - Excluded parent



Appendix I: Proposed Exclusion Resolution Templates

Facilities and certain personnel may need to fill out an Exclusion Resolution to exclude certain identified parties from access to classified information. The Defense Counterintelligence and Security Agency (DCSA) does not have official Exclusion Resolution templates; however, the following are being provided as a means of assisting industry and outside government stakeholders in ensuring all required information is reflected in Exclusion Resolutions for different scenarios.

I.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 "32 Code of Federal Regulations Part 117, [National Industrial Security Program Operating Manual \(NISPOM\) Rule.](#)"

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: 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)."



1.2 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 "32 Code of Federal Regulations Part 117, [National Industrial Security Program Operating Manual \(NISPOM\) Rule.](#)" In lieu of a Facility Security Clearance, *(Insert Name of Highest Tier Excluded Entity)* will report any changed conditions within the complete organizational structure that may impact the FCL eligibility, as defined in 32 CFR 117.9(c), 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 Counterintelligence and Security Agency.

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

Signature



I.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 Board)* 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 "32 Code of Federal Regulations Part 117, [National Industrial Security Program Operating Manual \(NISPOM\)](#)."

Signature _____
(Senior Management Official of LLC Member)

Date _____



I.4 Exclusion Resolution for Certain Directors, Officers, and LLC Member or Manager (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