NPS-CM-24-003

ACQUISITION RESEARCH PROGRAM
SPONSORED REPORT SERIES

Industrial Security as A Barrier to Non-Traditional Vendor Participation

December 2023

LCDR Stephen L. Astafan, USN
LT Michelle S. Browning, USN
MAJ Brent W. Bushong, USA
LCDR Geoffrey S. Rienstra, USN

Thesis Advisors: Dr. Nicholas Dew, Professor
Dr. Robert F. Mortlock, Professor

Department of Defense Management

Naval Postgraduate School

Prepared for the Naval Postgraduate School, Monterey, CA 93943

ACQUISITION RESEARCH PROGRAM
DEPARTMENT OF DEFENSE MANAGEMENT
NAVAL POSTGRADUATE SCHOOL

The research presented in this report was supported by the Acquisition Research Program of the Department of Defense Management at the Naval Postgraduate School.

To request defense acquisition research, to become a research sponsor, or to print additional copies of reports, please contact the Acquisition Research Program (ARP) via email, arp@nps.edu or at 831-656-3793.

Acquisition Research Program
Department of defense management
Naval Postgraduate School

ABSTRACT

The Department of Defense (DoD) aims to increase small business participation within the industrial base and has boosted its involvement in providing goods, services, and research and technology to support national defense. However, significant obstacles persist that dissuade non-traditional vendors from entering the defense ecosystem of contracting and acquisition. Prominent among them is the complex industrial facility security clearance (FCL) process.

Our research seeks to utilize discussions, data analysis, and validation from a trusted network to identify and remove industrial security process obstacles that dissuade non-traditional vendor participation and engagement within the DoD for classified projects. We discovered that a convoluted process, disaggregated resources, outdated policy, governmental-specific jargon, and a too-common tendency for smaller companies to work for larger prime contractors all reduce small businesses' desire to produce on the government's behalf. The outcomes of this research provide a three-tiered solution consisting of process, technical, and policy recommendations that streamline the application and provide a simple-to-understand framework for small business industrial clearance application and approval that fosters a more inclusive and diversified industrial base in support of national defense.

THIS PAGE INTENTIONALLY LEFT BLANK

ABOUT THE AUTHORS

LCDR Stephen Astafan a native of Winter Park, Florida, Lieutenant Commander Astafan graduated from Florida State University in 2012 with a Bachelor of Arts in International Affairs and Economics before receiving his commission via the Naval Reserve Officer Training Corps unit at Florida A&M University. In December 2014, he was assigned to Forward Deployed Naval Forces Japan aboard USS ANTIETAM (CG 54) as the Sales Officer and Food Service Officer. Ashore, Astafan joined the Navy Supply Corps School (NSCS) Newport, RI staff in 2017. At NSCS, he was the Department Head for the Leadership and Management Curriculum and Food Service Instructor for the Basic Qualification Course (BQC). In August 2019, he reported as the Supply Officer aboard USS JOHN PAUL JONES (DDG 53), homeported in Pearl Harbor, Hawaii. Following graduation from Naval Postgraduate School, he will report to NAVSUP Weapons System Support, Philadelphia, PA.

LT Michelle Browning is a Surface Warfare Officer. She commissioned from the United States Naval Academy is 2017 with a Bachelor of Science in political science. She served through deployment on USS Nitze (DDG 94) for her first division officer tour followed by serving as the Training Officer onboard USS Stethem (DDG 63) during her second Division Officer Tour. Upon graduating from the Naval Postgraduate School with a degree in Acquisition program management, she will be reporting to Surface Warfare Officer School, Department Head Class 281.

MAJ Brent Bushong was commissioned from Oregon State University in 2011. After graduation, he served as a Platoon Leader and Executive Officer in the 3rd Brigade 1st Armored Division as an Infantry Officer. During his tenure, he deployed to Afghanistan in 2014 to support Operation Enduring Freedom. His second assignment was at Fort Drum, NY, where he served as a Company Commander with the 2nd Battalion 22nd Infantry regiment. In his third assignment, he was an instructor for the Army ROTC program at Texas A&M University. Following his assignment at Texas A&M University, he was selected to become an Acquisition officer and chosen to attend the Naval Postgraduate School. He married his Wife Ciara in 2011 and is expecting to

have a baby boy in March 2024. After graduation in December 2023, he will report to Fort Eustis, VA, for his first Army Acquisition assignment.

LCDR Geoffrey Rienstra was raised in the city of San Antonio, Texas. He attended the University of Texas at Austin, where he received a BA in Government, graduating in 2009. He received his commission from Navy Officer Candidate School in December of 2012. After attending Navy Supply Corps School in Newport, RI, he reported to USS John Paul Jones (DDG 53), homeported in Pearl Harbor, HI. In April 2016, he reported to Navy Cargo Handling Battalion-1, Williamsburg, VA as a Transportation Intern and Battalion Supply Officer. In February 2018, LCDR Rienstra deployed with Naval Mobile Construction Battalion-11 to Rota, Spain as the Battalion Supply Officer. In March of 2019, he checked aboard USS STERETT (DDG 104), homeported in San Diego, CA. Following graduating from the Naval Postgraduate School, he will be report as the lead planner to COMLOGWESTPAC, Singapore.

ACKNOWLEDGMENTS

We greatly appreciate the efforts of our advisors, Professors Nick Dew and Bob Mortlock, for their unwavering support and guidance through the capstone process. Their mentorship has been invaluable, and their insights were vital to charting the course of this initial pilot of the NPS innovation capstone.

Dr. Erika Hussey of the Defense Innovation Unit played multiple roles during this research project, first and foremost as the topic sponsor who heard the protests of small business leaders with a desire to serve the government and decided to help. She also served as an enthusiastic mentor and coach; her expertise in small business, and communications, and her drive to identify and break down barriers is unmatched. She also managed to keep us on task and engaged, which was an awe-inspiring feat. We could not have done it without you.

To David Schiff and Javier Gomez of the National Security Innovation Network, your willingness to connect us with resources and contacts on both sides of the issue and provide stick and rudder feedback throughout the process was critical to our success. Thank you.

We sincerely thank all the government and small business leaders, industry and security experts, and innovative thinkers who took time out of their busy lives to participate in discussions and interviews for this study. Your knowledge, feedback, and validation were vital in assisting us in identifying problems and recommending solutions. Your willingness to share your experiences throughout the security process provided perspective on the challenges faced on both sides of the problem. We hope our efforts can alleviate some pain and shave some time off the process. To our families, we are profoundly grateful for your patience, understanding, and encouragement in supporting our transition from operational warriors to warrior scholars and all that entails. Your support has been, and will continue to be, the foundation of our success.

THIS PAGE INTENTIONALLY LEFT BLANK

NPS-CM-24-003

ACQUISITION RESEARCH PROGRAM
SPONSORED REPORT SERIES

Industrial Security as A Barrier to Non-Traditional Vendor Participation

December 2023

LCDR Stephen L. Astafan, USN
LT Michelle S. Browning, USN
MAJ Brent W. Bushong, USA
LCDR Geoffrey S. Rienstra, USN

Thesis Advisors: Dr. Nicholas Dew, Professor
Dr. Robert F. Mortlock, Professor

Department of Defense Management

Naval Postgraduate School

Prepared for the Naval Postgraduate School, Monterey, CA 93943

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

BLM	build, measure, learn
BRIDGES	bringing classified innovation to defense and government systems
CDaaS	Classified Desktop as a Service
CNC	computerized numerical control
CSA	Cognizant Security Agency
DARPA	Defense Advanced Research Projects Agency
DCSA	Defense Counterintelligence Security Agency
DISA	Defense Information System Agency
DIU	Defense Innovation Unit
DoD	Department of Defense
ECA	External Certificate Authority
EVS	Entity Validation System
FCL	Facility Clearance
FFL	federal firearms license
FOCI	foreign ownership control or influence
FSO	facility security officer
FY	fiscal year
GCA	Government Contracting Agency
IT	information technology
ITPSO	Insider Threat Programs Senior Official
KMP	key management personnel
NASA	National Aeronautical and Space Administration
NDAA	National Defense Authorization Act
NISP	National Industrial Security Program
NISPOM	National Industrial Security Program Operating Manual
NISS	National Industrial Security System
NISPOM	National Industrial Security Program Operating Manual

NSIN	National Security Innovation Network
OSBP	Office of Small Business Programs
PCL	personal clearance levels
PKI	public key infrastructure
POC	point of contact
PTAP	Procurement Technical Assistance Program
R&D	research and development
SAM	System for Award Management
SDVOSB	Service-Disabled Veteran-Owned Small Business
SMO	Senior Management Official
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment

EXECUTIVE SUMMARY

The purpose of this research is to meticulously identify and analyze the industrial security process obstacles that impede non-traditional vendor participation within the Department of Defense (DoD) for classified projects. By focusing on the intricacies of the current clearance process, this study aims to develop a streamlined, user-friendly framework to facilitate small business industrial facility security clearance (FCL) application and approval. The envisaged framework seeks to mitigate the barriers posed by cumbersome procedures, disaggregated resources, outdated policies, governmental-specific jargon, and financial barriers, enabling small businesses to navigate the clearance process more efficiently. Moreover, this research intends to foster an environment conducive to innovation and dynamic contributions by enabling small businesses to operate independently and reducing their reliance on prime contractor's sponsorship and clearances. The goal is to enhance small business participation in the DoD's industrial base, contributing to a more robust and diversified defense ecosystem.

To optimize and diversify participation within the DoD's industrial base, it is vital to recognize and address existing barriers faced by small businesses and non-traditional vendors. A significant portion of these challenges emanate from the industrial security clearance process, which can be particularly convoluted and daunting for newcomers in the defense contracting sphere.

Our recent research, backed by qualitative inquiry and discussions, centered on understanding this clearance process from the standpoint of small businesses, ones that have recently navigated through it, and the industry and security experts who oversee and manage the process. Our focus was to shed light on the multifaceted challenges posed by the existing systems — from disaggregated resources and outdated policies to intricate governmental jargon. Notably, the current system's capital-intensive nature often relegates small businesses to function under the umbrella of prime contractors, utilizing their clearances and facilities. This subservience creates a dynamic that stifles independent innovation and limits the number of participants and the breadth of contributions from these businesses.

The primary objectives of our research were as follows:

1. To identify the nuanced obstacles within the industrial security process that deter or delay small business participation through interviews and discussions with a trusted network of non-traditional vendors and industrial security experts.
2. To design a more accessible, streamlined framework for the clearance application and approval process, facilitating easier entry and independent operation for small businesses.
3. To map the facilities clearance process via the user journey of a first-time small business applicant to identify user pain points.
4. To recommend practical improvements divided among process, technical, and policy solutions.

Preliminary findings suggest that by reforming and simplifying the clearance process, the DoD can significantly enhance participation, fostering a more diversified industrial base crucial for national defense innovation. The outcomes of this study have the potential to shape policy adjustments and influence the broader strategy of the DoD in fostering a robust and diverse defense ecosystem that meets public policy goals and readiness requirements.

A. METHODOLOGY

In developing this Innovation Capstone Project methodology, we adopted an integrative approach, adapting Eric Ries's *Build, Measure, Learn* (Ries, 2011) framework initially for prototyping and adapting it and intertwining it with expert insights to comprehensively address small businesses' challenges in the DoD's industrial security clearance process. Initially, we formulated hypotheses pinpointing the core obstacles and developed a standard set of core research questions targeting government security experts and small business applicants. The first phase, focused on discussion was tailored to procure firsthand procedural knowledge, challenges, and suggestions regarding the process.

To effectively establish the extent and nuances of the issues, we conducted in-depth interviews with seasoned government security professionals, capturing their perspectives on policy intent, process complexities, and potential areas of improvement. Parallelly, we held discussions with a substantial cohort of small businesses ranging in size from five to 80,000 employees, gathering data on their specific impediments, capital-

intensive areas, and feedback on existing resources and policies. This dual-pronged approach ensured a broad yet detailed understanding of the landscape from both government and applicant viewpoints.

The next phase saw rigorous analysis to discern patterns, recurring themes, and underlying causes for the challenges highlighted by the participants. This iterative learning refined our initial hypotheses and informed the necessary adjustments to our user journey process map, ensuring our research methodology remained adaptive and robust. The culmination of these sequentially improved outcomes yielded a comprehensive three-tiered solution—encompassing process, technical, and policy recommendations—all aimed at streamlining the clearance protocol and fostering a more inclusive industrial base supporting national defense.

Additionally, a cornerstone of our methodology was incorporating a trusted network—a cultivated group of seasoned professionals, experts, and stakeholders deeply embedded within the government security and small business domains. This network served as a sounding board throughout our research, offering invaluable insights, validating findings, and presenting counter-perspectives that ensured a balanced viewpoint. Beyond data collection, the trusted network was pivotal in contextualizing the challenges within historical, procedural, and policy-driven frameworks. Their expertise enriched our research and provided nuanced understanding and credibility to the proposed solutions, ensuring they were practical and implementable within the DoD ecosystem.

B. PROBLEMS AND SOLUTIONS

Within the national defense and security framework, the Facilities Clearance process is instrumental in vetting businesses for their capability to handle classified information and bid on classified contracts. However, its procedural maze can be daunting for these same non-traditional vendors. This capstone project delves into critical challenges within the FCL procedure and proposes pragmatic solutions. Chief among these obstacles is the intricate nature of the FCL, which can be alleviated by mapping an individual user journey and refining the process. Furthermore, information fragmentation can be addressed by introducing a consolidated platform, which we have named

"TurboFCL." Biased language in FCL resources, leaning towards those with governmental backgrounds, can be neutralized with a universal literacy guide. An inherent subcontracting issue, where small businesses rely on prime contractors for sponsorship, necessitates a revised, direct engagement approach. Another paradox exists where businesses require sponsorship for a contract. Our research suggests that increasing the awarding of interim security clearances during contract solicitation could increase small business bids during contract solicitation. Additionally, while the FCL application does not have direct costs, indirect expenses, such as infrastructure and specialized personnel, can strain small businesses. Government-initiated financial aid can help in this regard. Additionally, considering the vastness of the Defense Counterintelligence and Security Agency (DCSA), restructuring specialized functions can streamline the process and enhance efficiency. By addressing these challenges, we can ensure that the FCL process promotes diversity and inclusivity in the defense ecosystem, optimizing innovation and national security.

The industrial security process, specifically the Facilities Clearance procedure, is a gateway for small businesses and non-traditional vendors seeking to contribute to the Department of Defense's classified projects. However, the current complexities surrounding the FCL process have stifled the potential of these key contributors. Our extensive research and interaction with governmental and small business stakeholders have illuminated the myriad challenges intrinsic to the FCL process. Our proposed solutions, from streamlining procedural steps to introducing platforms like "TurboFCL" and addressing financial burdens, serve as pivotal pathways to make the defense sector more attractive to private companies. Implementing these measures would facilitate the participation of a more comprehensive array of businesses and bolster national defense capabilities by tapping into a broader spectrum of innovative solutions. Ultimately, the goal is to craft an FCL process that is transparent, efficient, and conducive to the growth of a robust, diversified defense industrial base. Such an inclusive approach aligns with the DoD's mission and ensures that national security remains dynamic and resilient.

References

Ries, E. (2011). *The lean startup.* Crown Publishing.

I. INTRODUCTION

This research explores the numerous challenges faced by small businesses and non-traditional vendors aspiring to participate in the Department of Defense's (DoD) industrial base. The study focuses primarily on the impediments within the industrial security clearance process that deter vendor engagement in classified projects. Through comprehensive analysis and mapping of the current clearance process, this study identifies key obstacles, including disaggregated resources, outdated policies, complex government-specific jargon, and the capital-intensive nature of obtaining facility clearances. The ultimate goal of this capstone is to streamline the existing structures, proposing a coherent, simplified framework that can enhance small business participation and innovation in defense-related contracts and acquisitions by overcoming the identified barriers. The research's outcomes are expected to contribute significantly to policy reformation, fostering a more inclusive and diversified industrial base supporting national defense.

In the realm of national defense and security, the facilities clearance (FCL) process plays an essential role in ensuring that entities, particularly businesses, possess the requisite integrity and trustworthiness to access classified information, locations, and networks. While critically important for national security, this system can often become a labyrinth of procedures that are especially challenging for small businesses to navigate. This innovation capstone project seeks to delve into seven specifically identified problems these businesses may face and propose solutions that can help overcome them, fostering ease of entry and a broader defense ecosystem.

A. IDENTIFIED PROBLEMS AND SOLUTIONS

1. The Complexity of the FCL Process

Problem: For many small businesses, particularly those without a defense or government contracting background, the FCL process appears opaque and labyrinthine. They do not know where to start or how long it will take to finish. Throughout our research, we have discovered 11 significant processes involved with obtaining a facility clearance.

Solution: Undertaking a comprehensive mapping of the current FCL process can illuminate areas of unnecessary complexity and ambiguity. By understanding the process in-depth, we can identify bottlenecks, redundancies, and areas for process improvements, ultimately simplifying it for all applicants. Supplemental 1, the FCL Process Map, illustrates the steps that a business needs to undertake to obtain a facility clearance. The Appendix Facility Clearance Package and Supporting Processes Guide explains each step in plain language detail.

2. Fragmentation of Information

Problem: The information related to the facility clearance procedure is often scattered across various platforms, adding another layer of difficulty for businesses attempting to find cohesive guidance. For example, instructional guidance and documentation is spread across four different websites with 18 different instructional guides explaining various steps. To further complicate matters, some information can only be found by downloading specific documents to view the embedded attachments.

Solution: The proposed "TurboFCL" technical application could significantly reduce information disaggregation and confusion among resources for small businesses. By consolidating all relevant information, guidelines, and procedures into a single, user-friendly platform, "TurboFCL" can serve as a one-stop shop, drastically reducing businesses' time and effort searching for reliable information and repeatedly entering business data on multiple forms and applications.

3. Bias in Language and Presentation

Problem: The language used in training, instruction manuals, and the application process often leans towards those with prior security or governmental experience, inadvertently alienating a large pool of small business employees. The provided publications do not conform to the 2010 Plain Language Act or several presidential executive orders (Clinton, 1996; Obama, 2011; PlainLanguage, 2011). For example, the following excerpt from the FCL Handbook is quite challenging to understand for the typical small business owner, "Highest Cleared Entity Noting Excluded Entity's Exclusion and Resolution to Exclude Parent Organization" (DCSA, 2021). This type of

convoluted language could result in increased misunderstanding and errors with small businesses filing FCL package applications, thus increasing rejection rates and the administrative burden on DCSA adjudicators, compounding inefficiencies within the process.

Solution: Implementing a literacy guide that translates industry jargon and defense-specific terminology into plain, universally understandable language ensures that all businesses, regardless of their background, can approach the FCL process on equal footing. This inclusivity is paramount for a diverse defense industrial base.

4. The Subcontracting Conundrum

Problem: Many small businesses find themselves in a situation where they must start as subcontractors to secure sponsorship from a prime contractor. Prime contractor sponsorship of industrial security clearances potentially and questionably shifts an inherently governmental sponsorship responsibility onto for-profit agents (DCSA, 2021).

Solution: The government can directly engage with these non-traditional applicants by facilitating a more straightforward sponsorship process, especially for businesses seeking facility clearance. This approach can alleviate the indirect pressures on prime contractors and make the system more efficient. The government can create direct sponsorship programs.

5. The Contract-Sponsorship Paradox

Problem: Businesses need sponsorship for a contract, yet paradoxically, they often need to be awarded a contract to obtain the sponsorship required for a security clearance. In order to view classified solicitations posted by the government to bid on a contract, small businesses must already have a security clearance that is not granted without sponsorship.

Solution: Incorporating language within the National Defense Authorization Act (NDAA) to increase the utilization of interim security clearances during the solicitation application phase can bridge this gap. This provision will permit businesses to apply for contracts with the confidence that they can secure the necessary clearances post-award.

6. Financial Barriers

Problem: While the FCL process does not carry direct application costs, indirect expenses, such as hiring a facility security officer (FSO), ensuring a secure space, and required certifications, can be prohibitive for the smallest businesses. For example, the average salary of a Facility Security Officer is approximately $86,000/year per Glassdoor (Glassdoor, n.d.), and the average rental cost for a 1000-square foot commercial office space is roughly $38/sq. Foot, or $456,000/year, according to Commercial Edge's most recent quarterly report (Jozsa, 2023). Additionally, according to IdenTrust, the leading awarder of Public Key Infrastructure (PKI) certificates, it costs roughly $185 per year to maintain a PKI certificate (IdenTrust, 2022).

Solution: The government, recognizing the importance of a diverse defense industrial base, could offer financial assistance through grants, loans, or other funding mechanisms. Targeting non-traditional small businesses aiming to obtain facility security clearances, this financial support can level the playing field or lessen the initial financial hurdle, ensuring that the FCL process does not inadvertently favor only those with more significant cash flow.

7. DD254 Challenges

Problem: The DD254 is a pivotal document that validates a business's clearance to handle classified material. Our research indicates several challenges in both completing and managing this document. For businesses with multiple classified contracts, managing various contacts for each DD254 becomes complex, especially with personnel changes in government contracting agencies. This can result in communication gaps and project delays. For prime contractors, ensuring subcontractors comply with the DD254's security mandates is crucial, as non-compliance can halt work on classified projects. Furthermore, the current DD254 management system hampers collaboration. Companies frequently need to update the DD254 to include new personnel or stakeholders for classified discussions, slowing down the process and potentially delaying the delivery of vital capabilities to the warfighter.

Solution: Implementing the proposed "TurboFCL" technological solution can effectively address these challenges. Transitioning the DD254 to an online fillable application can mitigate communication issues and prevent potential delays arising from DD254 mismanagement. Such a platform would also expedite the process for companies needing to update personnel, physical locations, or stakeholders for collaborative efforts on projects. Additionally, an archiving library function would aid larger small businesses with managing multiple DD254s awarded to them.

The Facilities Clearance process, while critical for national security, should not become an insurmountable challenge for small businesses, which often bring fresh perspectives and innovative solutions. Addressing these identified problems with the suggested solutions can pave the way for a more inclusive, efficient, and diverse defense-industrial ecosystem. This inclusivity fosters innovation and strengthens national security by ensuring a broad, resilient spectrum of businesses contribute to the defense landscape.

THIS PAGE INTENTIONALLY LEFT BLANK

II. DISCUSSION QUESTIONS

This study addresses pivotal inquiries related to facility clearance procedures, viewed through the lens of small enterprises that have recently experienced them and from the industry and security specialists who administer them. Employing qualitative exploration and discussions with experts, we endeavor to understand the hardships encountered by small businesses during their progression through the security clearance process. The following questions were utilized to facilitate discussion:

1. Please give us a background on your company or agency, the number of employees, and your interaction with the industrial security process.
2. Describe the process for a facility security clearance as you understand it.
3. Where did you start this process/get the information to begin the process?
4. What were the significant hurdles and roadblocks you encountered throughout the process?
5. What changes to the process would make things easier for small businesses?
6. How long did it take to complete the security clearance process for your business? How long did you expect it to take?
7. What assumptions did you have going into the process? If so, did those assumptions change your approach? (timeline/personnel)
8. Were any specific references online or through other channels that made the process easier for you? Can you share those to aid our research?
9. Is the security clearance process a barrier to entry for small businesses?
10. Which branch of service do you have your security clearance with? If more than one, was the process different for different branches?
11. If you stopped the security clearance at any point, when and why did you stop?
12. Does your company have dedicated staff for this process?
13. What percentage of your business with the government requires a facility security clearance?
14. Regarding cyber security, have you ever heard of Project Spectrum?
15. How many hours did you or your staff dedicate to the facilities clearance process?
16. Do you know or have an estimate of how much money your business spent on gaining a security clearance?
17. What was the most challenging part of the clearance process?
18. If you could change the process, what would you change and why?
19. Can we use your responses in our capstone project and quote you directly?

20. Would you like to review and provide feedback on our facility clearance process map?

A. QUALITATIVE DISCUSSIONS, DATA ANALYSIS, VALIDATION

The methodology adopted for this capstone relied upon qualitative discussions, feedback, and validation provided by security experts, and non-traditional vendors specially tailored to meticulously map the user journey of non-traditional small businesses applying for facility clearances. This approach was paramount in achieving our overarching goal: to systematically unravel, understand, and subsequently enhance the clearance process that often appeared enigmatic to new entrants into the defense sector.

In the discussion phase, the focal point was mapping the user journey. The journey of a non-traditional small business applicant is inherently unique, often marked by an unfamiliarity with the defense ecosystem's intricacies. Hence, a holistic user journey was sketched, from the initial point of curiosity and exploration to the end goal of attaining a facility clearance. This included not just the initial recognition by the government as a small business entity or the primary FCL application process but the interconnected sub-processes, capturing the entirety of a newcomer's experience. A robust review of existing resources encompassed governmental guidelines (DCSA, 2023) and external aids like free government-provided training sessions (DCSA, 2022) and private paid consultancy services (FSO PROS, n.d.). Feedback mechanisms were instituted at each step to ensure this journey resonated with real-world experiences, paving the way for a dynamic and responsive mapping process.

The data analysis phase revolved around garnering feedback. Invaluable insights were gleaned by gauging users' perceptions, hurdles faced, and overall experience. This feedback was juxtaposed with the theoretical journey outlined in official guidelines, revealing the gaps between theory and practice. Benchmarking against the initial process map and leveraging real-world user journeys brought to light the discrepancies, inconsistencies, pain points, and areas for potential enhancement.

Transitioning to the validation phase, the gathered data was synthesized to discern areas necessitating overhaul or fine-tuning. While policy amendments were pivotal, two

primary innovations emerged: a plain language literacy guide and the "TurboFCL" platform. The former aimed at demystifying arcane jargon, rendering the application process more accessible to those without a defense or government background. The latter, "TurboFCL," addressed the pervasive issue of information fragmentation. By amalgamating all pertinent details onto a single platform, it offered small businesses a streamlined, coherent path to navigate the facilities clearance labyrinth.

The process map was refined with each iteration, ensuring the next cycle was built upon an even more robust foundation. Through continuous feedback loops and regular interactions with small business applicants and industrial security experts, each iteration became progressively more attuned to the real-world challenges and nuances of the facilities clearance application process. This iterative refinement did not just produce a process map; it created a living, evolving blueprint that could adapt and stay relevant amidst changing regulations, user needs, and industry dynamics.

Following is a sample of our application of methodology throughout the capstone:

1. Discussion

Map Initial User Journey: We outlined the basic steps that small businesses needed to undertake to apply for a facilities clearance and discovered separate processes that fed content into where we initially thought the process started. Then, we also had to map those earlier processes and assess how they connected to our origination point.

Reviewed Resources: Researched governmental guidelines, informational content, and support mechanisms, such as training and webinars or private consultation services, that assist businesses in understanding and navigating the application process.

Create Feedback Mechanisms: Established ways to gather user feedback at each step of the journey through discussions led by research questions to encapsulate resource usage, pain points, and obstacles.

2. Data Analysis

Gather Feedback: Collected data on users understanding of the process, challenges faced, and satisfaction levels at each step of the user journey.

Analyze Data: Reviewed the collected data to identify shared pain points, bottlenecks, and areas for improvement across multiple user experiences.

Benchmarking: Created the initial process map to measure the effectiveness of the application process as described in the official publications and utilized the experience of recent applicant's user journeys to seek feedback.

3. Validation

Identify Improvement Areas: Based on the feedback from small business applicants, we identified the areas in the user journey that could benefit from process improvements, did not match the prescribed procedures, or required additional support resources.

Update Resources and Processes: Make necessary recommendations for process and policy changes, additional support mechanisms, and potentially a newly developed and comprehensive application platform based on the learned insights, specifically the disaggregation of information.

Continuous Learning: Regularly reviewed the process and sought recommendation validation from government and industry experts, leveraging their skillsets to stay informed about any regulation changes or user needs to make ongoing improvements.

It is essential to highlight that once the feedback and learning from the first iteration of the process map had been applied to refine the user journey, the new journey and process map 2.0 became the baseline to build upon for the next version. Subsequent iterations focused on refining each stage of the user journey process map, continually improving the accuracy, clarity, and efficiency of the facilities clearance application process for small businesses based on the feedback from actual users and the validation of industrial security subject matter experts.

B. TRUSTED NETWORKS

Using a trusted network of companies and subject matter experts was crucial in navigating the complex industrial security landscape. This network of seasoned

professionals, industry veterans, and experts deeply embedded within government security and the small business domain acted as reservoirs of knowledge, experience, and firsthand information about the intricacies of the security clearance process and its obstacles.

One of the undeniable strengths of engaging with these trusted networks was the rich diversity of perspectives they offered. From companies that had successfully navigated the labyrinth of the FCL process and those that had quit to experts who had served on adjudication panels or developed policy guidelines, each brought a unique vantage point. This myriad of viewpoints ensured that our research was not just academically rigorous and accurate but also practically relevant and grounded in the realities of the field.

The mentorship provided by individuals within these networks was invaluable. New or inexperienced businesses often find themselves at a loss when confronted with the bureaucratic maze of clearance procedures. Having seasoned mentors who had "been there and done that" provided a guiding hand. They could highlight potential pitfalls, offer shortcuts, and even provide templates or sample documents, such as the Supplemental Sponsorship Template that had proven successful in past clearance approvals (Brown, 2023). This kind of mentorship significantly reduced the learning curve for our research, as it can for new businesses, making the entire process more accessible and less intimidating.

Additionally, the partnership opportunities that emerged from these networks were paramount. As was the case during our research, it can also benefit small businesses, especially those without experience in defense contracting, to partner with a company that has already been through the process. It offers credibility and legitimacy and provides practical benefits, like sharing compliance responsibilities, documentation, and infrastructural requirements like secure facilities. However, while the mentor-protégé relationship between contractors offers many benefits, the industrial security process's reliance on it highlights the complex and broken nature of the procedures and guidelines provided to newcomers.

Moreover, these trusted networks played a vital role in the iterative process of our research. As we mapped out the FCL process and identified potential bottlenecks and areas for improvement, feedback from the network was crucial. Their input allowed us to continuously refine our findings, ensuring that the proposed solutions were theoretically sound and practically implementable. The constant cycle of submitting, getting feedback, and refining was a cornerstone in ensuring the robustness of our research and, specifically, our process map.

In essence, while our research methodologies and analytical tools provided the framework for this study, the trusted networks breathed life into it. Their contributions, insights, and feedback ensured that our findings were comprehensive and grounded, offering solutions to bring real, tangible improvements in the facilities clearance process.

III. DISCUSSION PARTNERS

This section of the capstone report expounds upon the details of our trusted network of contributors from both government and industry. Their essential feedback and validation have been instrumental in shaping our findings and recommendations. Comprising defense officials, small business leaders, and industry experts, this collective has provided a holistic perspective on the challenges and potential solutions within the industrial security sphere. Their insights have not only enriched our understanding of the intricacies involved in managing classified work but have also grounded our process, technological, and policy proposals in practical, real-world experience. Below, we introduce and acknowledge these key players, whose collaborative input has been invaluable in our quest to streamline the security clearance process and enhance small business participation in national defense.

A. GOVERNMENT AGENCIES

1. Defense Innovation Unit

> The Defense Innovation Unit (DIU) strengthens national security by accelerating the adoption of commercial technology throughout the military and bolstering our allied and national security innovation bases (Defense Innovation Unit, n.d). DIU partners with organizations across the Department of Defense to rapidly prototype and field dual-use capabilities that solve operational challenges at speed and scale. With offices in Silicon Valley, Boston, Austin, Chicago, and inside the Pentagon, DIU is the Department's gateway to leading technology companies [nationwide]. DIU is the only DoD organization focused exclusively on fielding and scaling commercial technology across the U.S. military at commercial speeds. Working in six critical technology sectors, [their expert team] engages directly within the venture capital and commercial technology innovation ecosystem, many of which are working with the DoD for the first time. [DIU's] streamlined process delivers prototypes to our DoD partners and scalable revenue opportunities for our commercial vendors within 12 to 24 months. (Defense Innovation Unit, n.d).

2. National Security Innovation Network

> NSIN, the National Security Innovation Network, is an unrivaled problem-solving network in the U.S. Department of Defense that adapts to the emerging needs of those who serve to defend our national security

> (National Security Innovation Network, n.d). They are dedicated to bringing together defense, academic, and entrepreneurial innovators to solve national security problems in new ways. Our network is driven by the values of service, collaboration, and speed, creating exponential innovation. Together, the communities of defense, academia, and venture will drive the innovations that help us realize the better, safer, more robust world we want to build. (National Security Innovation Network, n.d)

3. Defense Counter-intelligence Security Agency

DCSA protects America's trusted workforce, trusted workspaces, and classified information (Defense Counterintelligence Security Agency, n.d.). To do so, they have two fundamental missions: personnel security and industrial security. Supporting these two core missions are counterintelligence and insider threat and security training. For over 50 years, the agency has used each of these missions to meet the threats of our nation's adversaries. DCSA is the largest investigative service provider in the federal government, supporting over 100 federal entities. They oversee 12,500 cleared facilities under the National Industrial Security Program (NISP). They ensure companies protect their facilities, personnel, and associated IT systems from attacks and vulnerabilities. (Defense Counterintelligence Security Agency, n.d.)

4. DARPA BRIDGES

> The BRIDGES initiative is a pilot effort sponsored by the Defense Advanced Research Projects Agency (DARPA) to connect innovation from small companies that traditionally do not work with the United States Government to classified Department of Defense (DoD) research and development (R&D) efforts (Defense Advanced Research Projects Agency, n.d.). Specifically, the goal is to connect innovators directly to the challenging problems in the classified realm and help develop solutions to those problems. BRIDGES aims to provide companies that demonstrate innovation and value to the DoD the means to obtain a facility clearance and interact directly with DoD customers at classified levels.
>
> To participate in BRIDGES, companies can submit short proposals against topic areas provided by the government…indicating what value they could bring to that area. The government will review all proposals, evaluate them, and invite selected companies to join the consortium, where each team within the consortium will be aligned to one of the topic areas. As a consortium member, a company will be sponsored for facility clearance and provided access to classified work areas and networks where they can perform classified work. They will also be invited to quarterly, in-person

meetings to interact with government personnel at classified levels. (Defense Advanced Research Projects Agency, n.d.)

5. Defense Information System Agency

The Defense Information Security Agency (DISA) is the nation's leading IT combat support agency (Defense Information Systems Agency, n.d.). They are a trusted entity responsible for connecting and safeguarding warfighters in the digital realm. Their role supports the joint forces' capabilities to prevail against adversaries, adapt to unforeseen changes, and maintain campaigns while staying prepared for future challenges. They "offer, manage, and ensure command and control, facilitating information-sharing capabilities through a globally available enterprise information structure" (Defense Information Systems Agency, n.d.). This infrastructure aids national leaders, military services, combat commands, and coalition partners across various stages, from competition to conflict. DISA's methods bolster the DoD's efforts, enhancing the security and robustness of networks and systems that fortify U.S. military advantages. Their strategic plan is a comprehensive blueprint to delve into emerging technologies and improve service delivery, aiming for a more secure, integrated, cost-efficient DoD IT architecture (Defense Information Systems Agency, n.d.).

6. Department of Defense Office of Small Business Programs

The DoD Office on Small Business Programs works diligently to optimize opportunities for small businesses, ensuring they play a pivotal role in strengthening national security (Office of Small Business Programs, n.d.). They aim to eQIP troops with robust combat power while bolstering the nation's economic prowess. Their vision centers around a unified group of small business experts who share core values and knowledge, collaborating closely with acquisition professionals. They engage small businesses that can fulfill the DoD's procurement necessities and bestow a competitive edge to Service Members. They manage funds for the small business program, ensuring efficient resource utilization, and actively evaluate and refine policies. They aim to maximize opportunities for small businesses within the DoD's procurement sphere. Their role also contributes to the DoD's acquisition strategy, ensuring small businesses have ample opportunities to offer innovative and competitive products and services.

Additionally, they set ambitious procurement goals for the DoD buying commands and actively monitor performance to achieve these targets (Office of Small Business Programs, n.d.).

7. Apex Accelerators

The APEX Accelerators, formally known as the Procurement Technical Assistance Program (PTAP), was authorized by Congress in 1985 to expand the number of businesses capable of participating in government contracts (APEX Accelerators, n.d.). The National Defense Authorization Act (NDAA) for FY 2020 ordered the PTAP to move to Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)), and the DoD Office of Small Business Programs (OSBP) began to manage and operate PTAP with a new name, APEX Accelerators, effective FY 2023. The APEX Accelerators program focuses on building strong, sustainable, and resilient U.S. supply chains by assisting various businesses that pursue and perform under contracts with the DoD, other federal agencies, state and local governments, and government prime contractors. (APEX Accelerators, n.d.)

B. PRIVATE COMPANIES

1. ABSI Aerospace & Defense

ABSI Aerospace & Defense is dedicated to offering swift acquisition solutions to aid program managers in providing the warfighter with vital technologies and training (ABSI Aerospace & Defense, n.d.). ABSI specializes in Manned and Unmanned Aviation Training, Test and Evaluation. They recognize the difficulties posed by the fast-paced requirements and the prolonged procurement process. They understand that quickly expiring non-program funds, which are challenging to execute, jeopardize programs and endanger lives. Having personally faced these challenges, they established ABSI Aerospace & Defense, driven by a genuine passion to address this issue. They hold multiple certifications, including being a Service-Disabled Veteran-Owned Small Business (SDVOSB) (ABSI Aerospace & Defense, n.d.).

2. Anduril

Anduril is a defense products company (Anduril, n.d.). Unlike most defense companies, they identify problems, privately fund their research and development and sell finished products off the shelf. Ideas are turned into deployed capabilities in months, not years, saving the government and

> taxpayers money—pioneering solutions for the software-defined conflicts of tomorrow. The next generation of military technology will depend less on shipbuilding and aircraft design advances than on software engineering and computing. Unlike traditional defense contractors who focus primarily on hardware, Anduril's core system is Lattice OS, an autonomous sensemaking and command and control platform that serves as the core platform for their suite of capabilities. They support operations with the U.S. Department of Defense, the U.S. Department of Homeland Security, the Australian Defense Force, the UK Ministry of Defense, and other partners worldwide. (Anduril, n.d.)

3. Collins Aerospace

Collins Aerospace is a pioneering force in the aerospace industry (Collins Aerospace, n.d.). They collaborate closely with customers and partners to design and implement innovative solutions that are reshaping the future of aerospace. Crossing market boundaries and disciplines, they introduce advanced technologies and turn groundbreaking aerospace concepts into reality. Their expertise spans a range of areas, from enabling hybrid-electric propulsion for fuel efficiency and crafting lighter and more efficient structures to reducing pilot workload through autonomous operations. They also focus on enhancing cabin experiences with modern design, harnessing data for insightful airline operations, and delivering digital systems for connected airspace. Recognizing the importance of each component in the bigger picture, they ensure everything works harmoniously. Their collaboration extends across Raytheon Technologies, where they continuously innovate, transforming ideas into cutting-edge solutions for current and future aerospace challenges (Collins Aerospace, n.d.).

4. Hermeus

> Hermeus was founded in 2018 with the mission to accelerate air travel radically (Hermeus, 2023). Using lessons learned from our time at space companies, they are developing Mach 5 aircraft to connect people faster and bring much-needed innovation to commercial flight. At Mach 5, more than twice the speed of the supersonic Concorde, passengers can cross the Atlantic in 90 minutes. On the path to hypersonic passenger aircraft, Hermeus is partnering with government agencies, including the U.S. Air Force and NASA, to develop a series of autonomous aircraft that de-risk the technology and solve urgent national security challenges. These products provide the data and confidence necessary to certify, produce,

operate, and maintain safe and comfortable commercial aircraft. (Hermeus, 2023)

5. MetaSCIF

MetaSCIF, Inc. is an innovative National Security technology company focused on creating revolutionary security technologies and solutions that simplify and scale classified access and protect America's technological advantage (Verbout, 2021). They design, build, and manage state-of-the-art classified GovCloud technology suites and innovative classified facilities that provide classified network access to cleared workplaces in America. MetaSCIF is targeting an immediate and growing gap in security by disrupting the traditionally expensive and cumbersome process of gaining secure facility and network access so that Defense and Intelligence innovation partners can protect people, systems, and data. Their novel facilities, diverse classified networks, and managed Classified Desktop as a Service (CDaaS) product lines offer clients secure, capable, and scalable classified access anywhere in America (Verbout, 2021).

6. Nooks

Nooks is a pioneering private venture founded by veterans deeply rooted in national security, bringing a wealth of experience from years of dedicated service to their country (Nooks, 2023). Recognizing the significant gap between the fast-evolving technology industry and the often slower-paced federal agencies, they understood that bureaucratic red tape hindered the government from accessing the best technologies and technology companies. These limitations were curbing the speed of innovation and tech adoption crucial for national security. Nooks was conceived in 2021 to fill this gap based on their in-depth knowledge of the defense innovation sector. They aim to provide turnkey classified environments near the point of need, all while ensuring an unmatched customer experience. (Nooks, 2023)

7. Radical Firearms, LLC

Radical Firearms is a distinguished Title II National Firearms Act Gun Manufacturer based in Texas (Radical Firearms, n.d.). They offer a comprehensive and ever-expanding range of Armalite-style silencers and machine guns. Not just an assembly

shop, they are a genuine manufacturer with a state-of-the-art machining facility where they produce custom-built rifles and silencers in-house. Many of their dedicated and passionate employees are veterans, a testament to their preference for hiring those who have served.

Starting as a hobby in a modest retail space, they initially handled federal firearms license transfers and crafted high-end rifles for discerning buyers. Their growth trajectory saw them incorporating more expertise, investing in computerized numerical control (CNC) machines for precision manufacturing, and expanding their passionate workforce. This evolution enabled them to produce parts cost-effectively, passing on significant savings to their customers. Today, they cater to a broad audience, from Military and Law Enforcement to 3Gun enthusiasts, offering top-tier firearms at competitive prices (Radical Firearms, n.d.).

8. Wise Engineering Consulting, LLC

Wise Engineering strives to be the DoD's subject matter experts in Weapon Systems Integration, specializing in the AEGIS Weapon System (Mehls, n.d.).

THIS PAGE INTENTIONALLY LEFT BLANK

IV. PROCESS-ORIENTED RECOMMENDATIONS

In the context of the creation of the Facilities Clearance process map (Supplemental 1) and creating the step-by-step walkthrough (Appendix 1), the following recommendations are proposed to refine the FCL Package application process, with an emphasis on enhancing efficiency and responsiveness for all stakeholders:

A. PRIMARY PROCESS RECOMMENDATIONS

(1) Recommendation 1

DCSA should consider eliminating or separating the sponsorship step from the FCL procedure. Instead, new business applicants should be mandated only to provide a completed DD254 form as a rationale for necessitating access to classified material. By entrusting businesses with the responsibility of supplying DCSA with the requisite data, the direct administrative involvement of an external sponsor can be reduced. Implementing this recommendation could lessen the application timeline by a window of 15 to 30 business days. This could simultaneously alleviate the responsibilities shouldered by sponsors and the administrative burden on DCSA by requiring only one document to initiate the FCL procedure.

(2) Recommendation 2

Post contract award with a Government Contracting Agency (GCA), businesses should be granted access to the National Industrial Security System (NISS). This would allow companies more time to fill out and provide the documentation required for an FCL package.

(3) Recommendation 3

When a company is contracted with a GCA, allow it to apply for PKI certification. This would reduce the number of companies that request an immediate follow-on extension of 14–21 business days during the FCL submission process.

(4) Recommendation 4

Once official sponsorship is approved, companies should be able to forward key management personnel (KMP) fingerprints alongside eQIP updates pertinent to clearances. This could expedite the overall process timeline by approximately 14 business days.

B. ADDITIONAL PROCESS RECOMMENDATIONS

(1) Recommendation A

DCSA should add an Appendix of example business documentation to the FCL Orientation Handbook. Incomplete or missing business documentation is the number one reason for FCL package rejection. If DCSA provided an example of each document type, this could reduce the number of rejections and reapplications, saving time for reviewers and applicants.

(2) Recommendation B

Increase the funding for DCSA to allow for the hiring of 50 new employees. These employees can act as case managers and would be assigned to a company at the beginning of the process to help it navigate the FCL process. This will lead to fewer rejected FCL applications due to DCSA employee involvement that incentivizes helping companies gain an FCL. This also allows for more communication between the company and DCSA.

(3) Recommendation C

The DCSA should consider the design and dissemination of model FCL packages tailored to various business types. Providing templates to businesses during their documentation preparation phase would provide them with a benchmark, ensuring alignment with established standards and thus minimizing initial submission rejections.

Reviewing the FCL Package application process recommendations, we identify significant potential for time savings and efficiency improvements. Removing or separating the sponsorship step can shorten the process timeline by 15 to 30 days. Allowing early PKI certification and the prompt forwarding of KMP fingerprints can cut

14–21 days and 14 days, respectively. Cumulatively, these changes can speed up the process by 40 to 65 business days. Additionally, with other recommendations targeting a reduction in package rejections, we see a clear path to making the FCL process more streamlined and accessible for new businesses. Implementing these changes will improve efficiency and expand entry into the defense industry to a broader range of enterprises.

THIS PAGE INTENTIONALLY LEFT BLANK

V. TECHNICAL WIREFRAME RECOMMENDATIONS

A. "TURBOFCL": REVOLUTIONIZING THE FACILITY CLEARANCE PROCESS

In today's rapidly evolving digital era, the seamless integration of technology into bureaucratic processes is not just a luxury but a necessity. DCSA, responsible for overseeing the FCL process, stands at a crossroads where the marriage of technology and procedure can significantly enhance efficiency and user experience. Enter the concept of "TurboFCL," a proposed application inspired by the success of platforms like Turbo Tax. This section delves into how such an app can radically streamline the facility clearance process, making it more accessible, efficient, and user-friendly.

B. THE ONE-STOP INFORMATION HUB

Navigating the maze of the FCL process can be daunting, especially for newcomers. An app like "TurboFCL," owned and maintained by DCSA, would consolidate all pertinent information, guidelines, FAQs, and resources. A centralized platform ensures applicants access to up-to-date, accurate, and comprehensive data, significantly reducing the chances of errors or misconceptions. This not only aids applicants but also reduces the administrative burden on DCSA, as they deal with fewer erroneous or incomplete applications.

C. SIMPLIFYING COMPLEX PROCEDURES WITH INTUITIVE QUESTIONS

Drawing inspiration from Turbo Tax, "TurboFCL" could break down the intricate FCL application into easy-to-understand questions. Instead of expecting the applicant to be familiar with industry jargon or specific requirements, the app guides them through every step. By converting complex procedures into layman-friendly queries, "TurboFCL" ensures that even those with minimal knowledge of the clearance process can confidently navigate and produce an accurate and quickly adjudicated application.

D. AUTO-POPULATION AND REDUCTION OF REDUNDANCIES

One of the significant challenges in any bureaucratic process is redundancy. Applicants often enter the same information on multiple forms or sections, such as Sam.gov, the sponsorship form, and the facility clearance application. "TurboFCL" can eliminate this tedious aspect by auto-populating data across all required fields and forms based on the user's input. Not only does this save time and reduce the chances of inconsistent data entries, but it also enhances the user experience.

E. REAL-TIME APPLICATION STATUS UPDATES

The waiting period after applying, often filled with uncertainty, can be anxiety-inducing for many. "TurboFCL," with its integrated system, could offer real-time status updates on the clearance process. Applicants can access their application's progress instantaneously whether it is under review, requires additional information, or has been approved/rejected. This transparency fosters trust and allows applicants to plan accordingly.

F. USER ACCESSIBILITY

The success of "TurboFCL" relies upon user-centric design. It must transform the complex and intimidating process of obtaining a facility clearance into an accessible and even empowering task for non-traditional small businesses. "TurboFCL" can emulate the success of platforms like Turbo Tax by prioritizing user experience. The app can democratize the facility clearance process with features like a user-friendly interface, integrated help options, and perhaps even AI-driven assistance.

The proposed "TurboFCL" app represents the future of administrative processes in the digital age. By integrating technology effectively, DCSA can streamline the facility clearance process and make it more inclusive and accessible. Such an initiative would testify to the agency's commitment to efficiency, transparency, and user-centric service. As the defense sector evolves, embracing technological solutions like "TurboFCL" will be crucial in maintaining agility, inclusivity, and excellence.

VI. POLICY RECOMMENDATIONS

Our research outlines a two-pronged strategy for policy recommendations – primary recommendations aimed at immediate impact and secondary recommendations for long-term structural change. The primary recommendations focus on enhancing the resources for the Defense Counterintelligence and Security Agency and the Defense Innovation Unit, advocating for the broader use of interim FCLs to expedite market entry for small businesses, and proposing financial mechanisms to support non-traditional vendors. Secondary recommendations include the integration of a digital platform, "TurboFCL," to streamline the clearance process, and establishing an FCL appeals process akin to that for individual security clearances. These recommendations are poised to address the current challenges faced by small businesses. They are designed to inject agility, transparency, and efficiency into the FCL process, thereby fostering a more robust and innovative defense industrial base.

A. PRIMARY POLICY RECOMMENDATIONS

1. Recommendation 1: Increased Resourcing to DCSA

> Fully resource and drive the Defense Counterintelligence and Security Agency to streamline processes, increase staffing, and pursue novel approaches to reduce the large backlog of individual and facility security clearances that impose long delays on contractors to begin work or scale. (Lofgren & al., 2023)

Additional funding should be allocated to DCSA to support the hiring of specialized case managers who can offer personalized assistance to small businesses (Lofgren et al., 2023). A certification program, developed in collaboration with the DoD OSBP, would ensure these managers are well-equipped to address the unique challenges small businesses face during the FCL process.

With dedicated case managers, small businesses can receive one-on-one guidance tailored to their specific needs and challenges. With a devoted point of contact, issues or questions can be addressed more quickly, reducing delays and errors in the FCL process. A dedicated liaison can build trust between OSBP, DCSA, and small businesses, fostering a more collaborative relationship that facilitates repeat contract participation

and the growth of small business participants within the defense industry. By serving as a feedback channel, the liaison can help DCSA identify areas for improvement in the FCL process based on small business experiences, leading to continuous enhancements tailored to the needs of non-traditional vendors.

Enhanced funding would lead to more efficient processing of applications, reducing backlogs and expediting the clearance process. It would also encourage greater participation from small businesses in the defense industry, fostering competition and innovation.

2. Recommendation 2: Increase Utilization of Interim FCLs

Interim FCLs allow small businesses to enter the defense market rapidly. By granting eligibility for access to classified information temporarily, these businesses can participate in the solicitation process without the lengthy wait for complete clearance processing. This can be particularly advantageous for projects with urgent timelines or industries where technological innovation outpaces the clearance process.

The National Industrial Security Program Operating Manual (NISPOM) permits the Cognizant Security Agency (CSA) to grant interim FCLs at its discretion, allowing temporary access to classified information pending the completion of full clearance processing (Defense Security Service, 2016). This provision could be utilized advantageously to assist small businesses eager to contribute to defense projects without the protracted wait times typically associated with the entire clearance process.

The NISPOM's guidance on interim clearances serves a dual purpose: it protects sensitive information while facilitating the defense industry's operational needs (Defense Security Service, 2016). By enabling small businesses to bid on contracts during the interim clearance phase, the Department of Defense harnesses a wealth of innovative solutions that might otherwise be sidelined. Interim clearances can level the playing field by allowing smaller entities to compete with larger, established defense contractors. This can lead to a more diverse and competitive market, which is beneficial for the DoD in terms of both cost and innovation.

The stringent requirements for interim clearances reflect a controlled approach to risk management. The manual underscores the need for a rigorous process that secures national security information while enabling qualified entities to access it as necessary. The procedures within the NISPOM regarding interim clearances are already robust enough to mitigate the risks associated with granting the increased total number of clearances (Defense Security Service, 2016).

However, the complexity of the NISPOM also indicates a pressing need for the DoD to improve outreach and education regarding interim clearances. Small businesses must be made aware of their availability, and DCSA must more greatly publicize and utilize the processes involved in obtaining them. Such efforts would ensure that the benefits of interim clearances are fully realized within the small business community.

The feedback from businesses via the case liaison officer, who navigates the interim clearance process, can also refine the NISPOM's procedures. This feedback loop is in keeping with the manual's commitment to continuous improvement and adaptation to the evolving needs of the defense sector.

The NISPOM already contains the necessary provisions for the increased use of interim FCLs and is a testament to the DoD's commitment to nurturing a capable and innovative defense industrial base (Defense Security Service, 2016). By granting small businesses quicker access to classified projects, the DoD not only empowers these businesses but also ensures that a wide array of technological and service-oriented solutions bolsters the nation's defense.

3. Recommendation 3: Grants, Loans, and Financial Considerations

The Defense Advanced Research Projects Agency (DARPA) has an initiative called BRIDGES, which stands for Bringing Classified Innovation to Defense and Government Systems (Defense Advanced Research Projects Agency, n.d.). DARPA states that this initiative is "a pilot effort to connect innovation from small companies that traditionally do not work with the United States Government to classified DoD research and development efforts." (Defense Advanced Research Projects Agency, n.d.) Their aim

is to leverage the agility and creativity of such companies and integrate their innovative technologies into the classified sectors of defense and government systems.

The BRIDGES initiative is particularly significant because it represents a concerted effort to bridge the gap between non-traditional vendors without clearances and the classified work crucial for national security. These small businesses often drive innovation due to their flexibility and cutting-edge technologies. However, they may lack the resources or knowledge to navigate the complex process of obtaining security clearances or meeting the stringent requirements of DoD contracts. Part of BRIDGES is to provide funding during the facility clearance process. This funding does not have to be in the form of a grant, and it could also be in the form of upfront contract financing to be considered part of the financial consideration upon completion of a contract (Defense Acquisition Regulations System, n.d.).

Increased funding for DARPA targeted explicitly toward the BRIDGES program could significantly build upon the DARPA BRIDGES model and encourage its transition to another resource sponsor because it would be difficult for DARPA to manage at a larger scale. Since "DIU's mission is to accelerate the adoption of commercial technology into the military and grow the national security innovation base" (Defense Innovation Unit, n.d) they may seem like a potential agency that could scale the BRIDGES model, however, while it is a rapidly moving contract sponsor, it is not the best-suited entity for classified systems, and does not sponsor enough contract actions per year to properly shepherd non-traditional vendors through the FCL Process. With funding targeted toward classified contracts, and a change to its charter however, DIU could expand its efforts to identify and contract with non-traditional vendors, similar to what BRIDGES is already doing within the classified space.

Additionally, creating a branch at DCSA in conjunction with DoD OSBP and the APEX Accelerator offices could localize grants and support at field offices, helping these vendors obtain the necessary industrial facility clearances while gaining tailored support toward entry into the classified contracting space. This support would not only expand opportunities for these companies within the classified contracting space but also enhance the innovation pipeline for the DoD by bringing in fresh perspectives and technologies.

B. SECONDARY POLICY RECOMMENDATIONS

1. Recommendation 4: Bringing the "TurboFCL" Application Into Policy

In today's digital age, an online portal or application can significantly streamline processes, reduce paperwork, and enhance user experience. For small businesses that may not have dedicated teams to handle FCL applications, an intuitive online portal can provide significant benefits and ease of use.

- A dashboard showing the application's current status.
- Automated notifications for any required actions or application status updates.
- A resource section with FAQs, video tutorials, guidelines, and checklists.
- A chatbot or live chat feature for immediate assistance.
- Secure document upload and storage capabilities.

This platform can reduce errors in application submission, decrease processing times, and provide businesses with a clear view of their application's progress. It can also reduce the administrative burden on DCSA and contract sponsors by automating specific processes and reducing the errors in package submissions that DCSA must adjudicate and reject.

Our research found that the complexity of the FCL process, fragmentation of information, and bias in both language and presentation could be solved by putting all the required FCL information into one portal for sources and applications. These problems identified by this study would be solved through small businesses having the ability to not only see all the information in one domain but to have the ability to learn through various training materials already on the application.

This model would significantly decrease the amount of time DCSA employees should have to spend adjudicating applications that are submitted wrong due to errors that small businesses did not understand or forms missing. However, upon creation, its use would have to be adequately supported within the policy framework of the NDAA, NISPOM, and DCSA publications.

2. Recommendation 5: Establish an FCL Appeals Process

Establishing an appeals process that mirrors the procedure for individual security clearances is a critical step toward fairness and transparency in the defense contracting arena.

Individuals can appeal security clearance denials, and it stands to reason that the same principles should apply to entities (DCSA, 2023). Aligning the FCL appeals process with individual clearances would quickly provide transparency and be easy to implement since the appeals framework already exists for personnel. An appeals process would provide companies with a formal avenue to contest adverse decisions, ensuring that all parties could present additional information or clarify misunderstandings from a convoluted procedure. This is a fundamental aspect of due process and is essential for maintaining trust in the system.

Mistakes can occur in the adjudication of clearances. An appeals process allows for correcting errors that might have been made during the initial review. This is particularly important for small businesses, where an FCL denial can have significant financial implications. An appeals process would help standardize responses to FCL denials. Currently, without a formal appeals process, responses to denials may vary, leading to inconsistencies and often a complete restart of the application process. A standardized process would ensure that all companies are treated equally and that decisions are made based on consistent criteria. It would also ensure that FCL packages are adjudicated at their current step, allowing for a continuation of the process without having to resubmit the entire package.

Thus, this clear and structured appeals process would increase the transparency of the adjudication process. Companies would have a better understanding of the reasons behind denial and the steps they can take to address the issues raised. This transparency is crucial for companies to make informed decisions about their involvement in defense contracts. This process benefits not only the companies involved but also DCSA by providing a feedback loop to learn from appeals and continuously improve their process based on common errors. This could lead to more accurate initial adjudications, fewer

erroneous application submissions, and fewer application re-submissions and appeals over time.

By allowing companies to appeal and potentially overturn unjust denials, the DoD can mitigate the risk of losing valuable and capable partners in the defense industrial base. This is especially important when considering the unique and innovative solutions that small businesses can provide. For small businesses, the denial of an FCL can be economically devastating. An appeals process provides a safety net that could help protect the economic viability of small businesses specializing in defense-related work.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX. FACILITY CLEARANCE PACKAGE AND SUPPORTING PROCESSES GUIDE

This appendix describes the Facility Clearance package and its supporting processes through the lens of a small business applicant. While researching the process that a small business undergoes to obtain an FCL, obstacles were identified that, if corrected, would yield process improvements, and increase non-traditional vendor participation in the Department of Defense. The Process Guide is intended to be utilized alongside the Process Map (Supplemental _FCL Process) for assistance in completing the below applications.

(1) Starting Out

To start this process, a business must desire to work with the government on any classified contract. That business will then go to the business.defense.gov website to start the journey. As the company loads the home page to the website, it will see several dropdowns across the top of the page. This is the next step in the process. Businesses must click the link to search for current opportunities (Office of Small Business, 2023).

(2) Sam.gov: Entity ID & CAGE CODE

Businesses will now need to register with Sam.gov. In the top right corner of the webpage is a box with register your entity or get a unique entity Identification. This is the next step in the process. First, businesses will need to create a login for Sam.gov. This will start the registration process. Companies must register to conduct business with the government, not just sign up for their entity Identification. When businesses click on "Get Started," they will be taken to another screen with a status bar showing the steps to completion for Sam.gov registration. Businesses will also be able to view the registration checklist. This checklist is 18 pages long and will provide information about the types of questions that businesses will be asked as part of their registration. The registration questionnaire is broken into eight sections with 130 questions based on the business responses. The sections are broken down into the following: Entity ID information, Core Data, Assertions, Representations and certificates, Architect and Engineering, FAR

supplement questions, Point of contact information, and Small Business Association supplement questions (U. S. General Services Administration, n.d.). Once businesses have completed the questionnaire and submitted it to Sam.gov, they will enter the entity validation process. The information provided to sam.gov via the entity questionnaire will be reviewed by the Entity Validation System (EVS). If EVS determines that all the information required is correct, the business will receive a unique entity ID and CAGE Code, usually within seven business days. EVS will contact the business if any information is incorrect and ask them to clarify or correct the data (Rollins, 2002). Once businesses have a unique entity ID and CAGE Code, they can review open solicitations on Sam.gov for a government contract. This will start the next step in the process, where either a business gets a contract from a government contracting agency or gets a contract working as a subcontractor under a prime.

(3) Sponsorship

Once a business is under contract or about to be under contract to work on a classified project for the government, it will undergo the process of sponsorship. This process will involve both the business and the sponsoring entity. The sponsoring entity can be a government contracting agency or a prime contractor with facility clearance and approval to work on the project in question. The first step is for the sponsoring entity to create an account with the National Industrial Security System (NISS) if they do not already have one (DCSA, 2020a). The sponsoring entity must go to the NCAISS homepage at the following URL: https://ncaiss.dss.mil/ to register for an account (DCSA, 2014). Once on the home page, a notice and consent to monitoring will appear. Once accepted, they must go to the bottom left of the homepage and click “register” for an account under self-enrollment. From here, new registers will be asked to provide their first and last name and email address, and then they will create a password. Following creating a username and password, they will generate challenge questions and answers. After completing the above, the sponsoring entity must review all the data to ensure it is correct, then continue to the privacy act statement. Once they have read the statement act and agreed to the terms, they will click “confirm” and submit their information to NISS. After submission, the user will be prompted to register their certificate; this refers to the

PKI certificate for DoD-approved users. If the user does not have a certificate or wishes to register their certificate later, they can skip this step. Now, the sponsoring entity can log into NISS. Once logged into the system, it will take you to the homepage of the Defense Security Service portal. On this portal, users will see the following: "My Information, My Applications, Request/modify/Access, Track Request, and Pending Approvals" (DCSA, 2020a). Users must click "Request/Modify/Access" to become a sponsor. Users will need to verify some basic information entered into the system as part of their registration. Then, they will see a started box labeled the NISS category. This is a drop-down box where the sponsoring entity must select a sponsor. Users must also provide their CAGE Code, role requested, and time zone, then move on to the next screen. This will take you to the submission screen. Users must verify that the data is correct, then click "confirm" on the bottom left corner. Once DCSA has approved the new role, the sponsoring entity can start the sponsorship form (DCSA, 2020a). The exact process discussed above for the sponsoring entity will be used by the small business later in the process when they have passed the sponsorship phase of the facility clearance process.

The sponsoring entity can now start the sponsorship form. Number four, under quick links on the home portal page of NISS, is the submit a sponsorship request button. Once the sponsoring entity clicks "request," a window with instructions will appear. The window will have six different tabs that are organized horizontally across the top of the window. These tabs include the following: "Instructions, Sponsored Facility Information, Business Information, FSO Information, Contract Information, Program-Specific GCA POC, and Sponsor Information" (DCSA, 2020a). Each tab has questions that must be filled out to submit the request to DCSA. Under the Facility information tab, the sponsoring entity must know the following information about the business it wishes to sponsor: Company legal name, Aliases used by the company, CAGE Code, Physical Address, and Company website. Under Business Information, the sponsoring entity must know the following: date of incorporation, state of incorporation, business structure, facility location, type of business, products, and services provided, and if they have ever held an FCL with another government agency besides DCSA. An example of this is if they had worked with the Central Intelligence Agency and were granted a facility

clearance to work on classified projects. Under the Facility Security Officer (FSO) information tab, the sponsoring entity will need to know the following information: "Full legal name of the sponsored FSO, Email address, phone number, work location (physical address, state, zip code), and an alternate point of contact if they have one (recommended)" (DCSA, 2020a). In the contract information tab, the sponsoring entity will need to know the following: "Prime contract number (this number should be the contract number that requires access to classified information), government customer, program name, level of clearance required, level of safeguarding required, total number of employees at sponsored facility, primary industrial base technology category applicable to the contract, Unclassified description of the type of information that the company will be required to access, and is the request based on a subcontract to the issued sponsored facility" (DCSA, 2020a). The next tab will be the program-specific government contracting agency (GCA) point of contact (POC). In this tab, the user will need to know the first and last name of the GCA POC, phone number, title, email address, and additional POC if necessary. In the previous tab, sponsor information, the sponsoring entity will provide information about themselves. This will include the sponsor's CAGE Code, first and last name of the sponsor, name of the company, title, and email address. The final step in sponsorship will be for the sponsoring entity to upload supporting documentation for DCSA to review. At a minimum, the DD254 (DoD form required to access classified information) will be completed and submitted. Additional documentation that can be uploaded includes the following: "compelling need letter, GCA concurrence letter, GCA written approval for per-award access, government installation letter, and the statement of work" (DCSA, 2020). After submitting a completed sponsorship package, a DCSA reviewer will be assigned to determine if the request is valid.

(4) Facility Clearance

Up to this point in the process, nothing is considered time-sensitive. However, once a business starts the facility clearance process, they are officially on the "clock." Day one of the Facility Clearance (FCL) process begins with an email from DCSA to the business. In this email, businesses will have a discontinuation date for a completed FCL

package 20 days from the date of the email, and businesses will have a discontinuation date for key management personnel (KMP) to complete their individual security clearance in e-QIPs as well as complete their fingerprints 45 days from the date of the email. In this email, businesses will have a list of resources with links to aid them in the FLC process. These resources include a link to the DCSA website for FCL orientation videos, the FCL orientation handbook, a list of approved vendors to get a public key infrastructure (PKI) certificate, and how to request an NISS account. Businesses are encouraged to begin by reviewing these resources provided. Once ready, the business can simultaneously apply for a PKI certificate and request a NISS account. Requesting a NISS account was discussed earlier under the sponsorship section. The steps the sponsoring entity took to gain a NISS account will be the steps a brand-new business must follow to acquire access (DCSA, 2020a). To gain a PKI certificate, users must click the link in their day one email, which will take them to the following website: https://public.cyber.mil/eca/. On this website, towards the bottom of the page, there will be a section with Approved ECA Vendors in purple letters. The two links below this section are the approved PKI vendors. Widepoint and Identrust, Inc. vendors provide similar services that meet the DoD external certification requirements (DISA, 2023).

(5) PKI

Widepoint offers three external certificate authority types: “medium assurance, medium token assurance, and medium hardware assurance” (WidePoint, 2023). All three have individual instructions to aid you with completion of the application form. Once the user has completed the application, they must send photocopies of two government-issued photo IDs and an organizational affiliation letter signed by the company via physical mail. Once Widepoint receives the application and photocopies, they will process your application within about ten business days. Businesses can pay for an expedited issuance for a fee of $49. Once Widepoint approves your application, they will mail the business its PKI certificate. Downloading certificates from the website finalizes the PKI procedure. Upon completing this, users should have a fully functional PKI certificate (WidePoint, 2023).

(6) PKI Continued

IdenTrust, Inc. is the other vendor businesses can utilize for PKI certifications. Upon clicking on the link at the bottom of the *public.cyerber.mil* website, users will be taken to the homepage of identrust.com. Businesses should scroll down to the middle of the webpage and see a button for buy now. This is where they will start applying for their PKI certificate through IdenTrust. Upon clicking "buy now," users will be taken to another webpage to select the DoD External Certificate Authority (ECA) program. After selecting their ECA program at the bottom, they will select "next." The website will then ask users if they reside in the United States and then ask them to select the number of years they will need this certificate and what kind of device they will require (Smart card or USB with token). Following that selection, users will fill out some questions regarding their business and personal information and then check out. After businesses have paid for the services, they must physically mail in photocopies of two government IDs. Once IdenTrust receives the photocopies, they will process your request within ten business days. Upon approval, the PKI certificate will be physically mailed to the business for them to load the certificate onto the USB or smart card upon receipt. After loading their certificates, businesses should have a fully functional PKI certificate (IdenTrust, 2022).

Now that businesses can access the NISS website, they can prepare their FCL package. Businesses will log into NISS and navigate to the dashboard section. They will then select Submit my FCL package number 11 on the drop-down menu. Once the user clicks "submit my FCL package," they will be brought to another screen. From there, they will select "Open my initial FCL package." This will redirect the user to the desired FCL package. Across the top of the screen, they will have five tabs: Basic Information, SF-328, Supporting documents, KMP list, and Industry-DSS package comments. Starting in the basic information tab, the following data will need to be provided: Company Name, CAGE Code, Business structure (can be prepopulated from the sponsorship packet), Tax ID, any legal names the company had previously, list of all addresses the company had, dates associated with name and address changes. Once the company has provided all the data required, it can move on to the next tab, SF-328 (DCSA, 2021).

(7) SF-328

Businesses will now move to the next tab, SF-328. There is an option for businesses with a branch or division office, and the parent company will submit the SF-328 on behalf of the branch or division office. For those businesses that the above does not apply to, they will answer ten questions regarding foreign ownership control influence (FOCI). The questions and the sub-questions are shown in Table 1. (SF 328 Questionnaire) and can be found in the FCL Orientation Handbook that DCSA provides. After completing the questionnaire, businesses must print a copy of the SF-328, have a designed witness sign, and then scan it back into the FCL packet for processing (DCSA, 2021).

Table 1. SF 328 Questionnaire. Source: DCSA (2021).

Question # 1A	Do any foreign person(s), directly or indirectly, own or have beneficial ownership of 5% or more of the outstanding shares of any class of your organization's equity securities? If yes:
	Identify the percentage of any class of stock or other securities issued that foreign persons own, broken down by country. Include indirect ownership through one or more intermediate level(s) of subsidiaries. Indicate the voting rights of each class of stock.
	Are there shareholder agreements? If yes, attach a copy(ies); if none, so state.
	Indicate whether a copy of the SEC Schedule 13D/13G report has been received from any investor. If yes, attach a copy(ies).
Question #1B	(For entities which do not issue stock): Has any foreign person directly or indirectly subscribed 5% or more of your organization's total capital commitment? If yes:
	Identify the percentage of total capital commitment to which foreign persons subscribe.
	Is there an agreement(s) with the subscriber(s)? If yes, attach a copy(ies); if none, so state.
Question #2	Does your organization, directly or indirectly through your subsidiaries and/or affiliates, own 10% or more of any foreign interest? If yes:
	Identify the foreign interest by name, country, percentage owned, and personnel who occupy management positions with the organizations.
	If there are personnel from your organization who occupy management positions with the foreign firm(s), identify the name(s), title, and extent of involvement in the operations of the organizations (to include access to classified information).

Question #3	Do any non-U.S. citizens serve as members of your organization's board of directors (or similar governing body), officers, executive personnel, general partners, regents, trustees, or senior management officials? If yes:
	Identify the foreign person(s) by name, title, citizenship, immigration status, and clearance or exclusion status.
	Attach copies of applicable by-laws or incorporation articles describing the affected position(s). However, if you have already provided such copies to the cognizant Security Agency Industrial Security Representative, so state.
Question #4	Does any foreign person(s) have the power, direct or indirect, to control the election, appointment, or tenure of members of your organization's board of directors (or similar governing body) or other management positions, or have the power to control or cause the direction of other decisions or activities of your organization? If yes:
	Identify the foreign person(s) by name, title, citizenship, and all details concerning the control or influence.
Question #5	Does your organization have any contracts, agreements, understandings, or arrangements with a foreign person(s)? If yes:
	For each instance, provide the name of the foreign person, country, percentage of gross income derived, and nature of involvement, including: -Whether defense/nuclear related or not -Involvement with classified or export-controlled technology -Compliance with export control requirements -Where the organization has a large number of involvements and where these involvements are not defense/nuclear-related and represent a small percentage of gross income, the explanation can be a generalized statement addressing the totals by country.
Question #6	Does your organization, whether as a borrower, surety, guarantor, or otherwise, have any indebtedness, liabilities, or obligations to a foreign person(s)? If yes:
	Provide your overall debt-to-equity ratio (in percentage).
	With respect to indebtedness or liability to a foreign person, indicate to whom indebted or liable, what collateral has been furnished or pledged, and any conditions or covenants of the loan agreement. If stock or assets have been furnished or pledged as collateral, provide a copy of the loan agreement or pertinent extracts thereof (to include procedures to be followed in the event of default).
	If any debentures are convertible, provide specifics.
	If loan payments are in default, provide details.
	This question should be answered in the affirmative if the debt is with a U.S. entity that is owned or controlled either directly or indirectly by a foreign person. If unknown, so state.
Question #7	During your last fiscal year, did your organization derive:

	5% or more of its total revenues or net income from any single foreign person.
	In the aggregate, 30% or more of its revenues or net income from foreign persons? If yes to either part of the question:
	Provide the overall percentage of income derived from foreign sources by country, nature of involvement, and type of services or products.
	Indicate if any single foreign source represents in excess of 5% of total revenues or net income.
	Indicate whether any classified information is involved.
	State whether the facility complies with applicable export control requirements.
Question #8	Is 10% or more of your organization's securities held in "nominee shares," in "street names" or in some other method that does not disclose the beneficial owner? If yes:
	Identify each foreign institutional investor holding 10% or more of the voting stock by name and address and the percentage of stock held.
	Indicate whether any investor has attempted to or has exerted any control or influence over appointments to management positions or influenced the organization's policies.
	Include copies of SEC Schedule 13D/13G.
Question #9	Do any of the members of your organization's board of directors (or similar governing body), officers, executive personnel, general partners, regents, trustees, or senior management officials hold any positions with, or serve as consultants for, any foreign person(s)? If yes:
	Provide the name, title, citizenship, immigration status, and clearance or exclusion status of all such persons.
	Identify, by name and address, each foreign organization with which such persons serve and indicate the capacity in which they are serving.
	Include a Statement of Full Disclosure of Foreign Affiliations for every cleared individual who is a representative of a foreign interest.
Question #10	Is there any other factor(s) that indicates or demonstrates a capability on the part of foreign persons to control or influence the operations or management of your organization? If yes:
	Describe the foreign involvement in detail, including why the involvement would not be reportable in the preceding questions.

(8) Supporting Documents

The next tab that businesses must tackle is the supporting documents tab. Under this tab, businesses will need to provide a Legal Organization Chart, DD Form 441, and required recorders, depending on the type of business structure. The Defense

Counterintelligence Security Agency lists the eight types of business categories as follows: “Sole Proprietorship, General Partnership, Limited Partnership, Joint Venture, Privately Held Corporation, Publicly Held Corporation, Limited Liability Company, and College/University” (DCSA, 2021). Table 2 (Business Records) is a recreation of the table in the FCL Orientation Handbook that DCSA provides. Once all documents have been uploaded, businesses can work on the next tab labeled KMP list (DCSA, 2021).

Table 2. Business Records. Sources: DCSA (2021).

Business Structure	Required Records
Sole Proprietorship	• Business License • Fictitious Name Certificate • Recent changes to the Company Structure
General Partnership	• Business License • Fictitious Name Certificate • Partnership Agreement • Legal Organization Chart • Board/Company Meeting Minutes • Recent changes to the Company Structure • FSO/ITPSO Appointment Letter • KMP Citizenship Verification • Signed undated DD Form 441 • Signed SF 328
Limited Partnership	• Business License • Fictitious Name Certificate • Partnership Agreement • Certificate of Limited Partnership • Legal Organization Chart • Board/Company Meeting Minutes • Recent changes to company structure • FSO/ITPSO Appointment Letter • KMP Citizenship Verification • Signed undated DD Form 441 • Signed SF 328
Joint Venture	• Business License • Fictitious Name Certificate • JV Agreement • Legal Organization Chart • Board/Company Meeting Minutes • Recent changes to the Company Structure • FSO/ITPSO Appointment Letter • KMP Citizenship Verification • Signed undated DD Form 441 • Signed SF 328
Privately Held Corporation	• Business License • Fictitious Name Certificate

Business Structure	Required Records
	• Articles of Incorporation • By-Laws • Stock Ledger • Legal Organization Chart • Board/Company Meeting Minutes • Recent changes to company structure • FSO/ITPSO Appointment Letter • KMP Citizenship Verification • Signed undated DD Form 441 • Signed SF 328
Publicly Held Corporation	• Business License • Fictitious Name Certificate • Articles of Incorporation • By-Laws • Stock Ledger • Most recent SEC filings • Legal Organization Chart • Board/Company Meeting Minutes • Recent changes to the Company Structure • FSO/ITPSO Appointment Letter • KMP Citizenship Verification • Signed undated DD Form 441 • Signed SF 328
Limited Liability Company	• Business License • Fictitious Name Certificate • Certificate of Formation or • Articles of Organization • Legal Organization Chart • Operating Agreement • LLC Meeting Minutes • Recent changes to company structure • FSO/ITPSO Appointment Letter • KMP Citizenship Verification • Signed undated DD Form 441 • Signed SF 328
College/University	• Charter • Board/University Meeting Minutes • Legal Organization Chart • Recent changes to university Structure • FSO/ITPSO Appointment Letter • KMP Citizenship Verification • Signed undated DD Form 441 • Signed SF 328

(9) KMP List

Businesses must now list all the required Key Management Personnel (KMP). This will change based on the structure of the business. Businesses may list additional personnel on this list but are only required to provide the data for their KMPs. Once on the KMP tab, businesses will click on the person who wishes to provide data, such as the company Facility Security Officer (FSO). A window will populate, and businesses can enter the following data: Prefix, First Name, Last Name, Middle Name, Social Security Number, and check a box if they are considered essential KMP members. Essential KMP Members include the FSO, the Insider Threat Programs Senior Official (ITPSO), and the Senior Management Official (SMO). Once the data is entered, the KMP member will populate as identified within the tab. Once all KMP members have been labeled as identified in the tab, businesses can move on to the next tab, Industry-DSS Package Comments (DCSA, 2021) Table 3, Key Management Personnel, shows KMP by business structure.

Table 3. Key Management Personnel. Source: DCSA (2021).

Business Structure	Required KMPs
Sole Proprietorship	• Owner of sole proprietorship • Senior Management Official • Facility Security Officer • Insider Threat Program Senior Official
General Partnership	• Senior Management Official • Facility Security Officer • Insider Threat Program Senior Official • All General Partners, except Single Partner (must be cleared) Management Committee (all committee members must be cleared)
Limited Partnership	• Senior Management Official • Facility Security Officer • Insider Threat Program Senior Official • All General Partners, except: Single Partner (must be cleared) Management Committee (all committee members must be cleared) • Limited Partners need PCL if they work on classified contracts or need access to classified information
Joint Venture	• Senior Management Official • Facility Security Officer

Business Structure	Required KMPs
	• Insider Threat Program Senior Official • JV Partners must be excluded or cleared if their duties require access to classified information. • Officials working on JV are cleared if their duties require access to classified information
Privately Held Corporation	• Senior Management Official • Facility Security Officer • Insider Threat Program Senior Official • Chairman of the Board • Vice Chair of Board, if provisions for rotating or Pro Tem duties • Corporate Officials are cleared if their duties require access to classified information
Publicly Held Corporation	• Senior Management Official • Facility Security Officer • Insider Threat Program Senior Official • Chairman of the Board • Vice Chair of Board, if provisions for rotating or Pro Tem duties • Corporate Officials are cleared if their duties require access to classified information
Limited Liability Company	• Senior Management Official • Facility Security Officer • Insider Threat Program Senior Official • LLC Members are cleared if their duties require access to classified information • Managers
College/University	• Senior Management Official • Facility Security Officer • Insider Threat Program Senior Official • President • Regents/Trustees/Directors are cleared if their duties require access to classified information

(10) Industry-DSS Package Comments

This tab is where businesses can enter any final comments for DCSA. Once complete, businesses must click "submit" at the bottom left of their screen. Should there be any errors or incomplete data, a screen will populate and show where there are deficiencies in their FCL package. Businesses will be allowed to fix any issues and then resubmit.

(11) DCSA Review

At this point, all documentation has been submitted to DCSA. Businesses will see that their FCL package is under review. If there are any issues, the reviewer will email instructions. If everything looks good, the FSO will get an email regarding submitting any personal clearance levels (PCL). This ensures that all KMP-listed personnel in the FCL package have the required security clearance. Any personnel that need a clearance will now start their e-QIP. Additionally, all personnel will submit fingerprints. Fingerprints can be submitted electronically via two different options. Option A is to submit an electronic fingerprint file to the Facility Clearance Branch via secure web fingerprint transmission. Option B submits electronic fingerprints via a third-party secure web fingerprint transmission account (DSS, 2014). A complete guide can be found on the DCSA website in the entity vetting "Facility Clearance & FOCI" section.

(12) On-site Inspection

The final step in the FCL process is the on-site inspection. Businesses must coordinate with the DCAS field officer to inspect their facility. The facility inspection has 234 different inspection requirements. Some requirements may not apply to particular businesses depending on various reasons. All facilities will have a minimum of 82 inspection points. These are the basic requirements listed in the Self-Inspection Handbook for National Industrial Security Program contractors. Section 3 lists all the questions/inspection points a business must pass. The basic section has seven main categories: Procedures, Reporting Requirements, Eligibility for Access to Classified Data, FOCI, Security Training and Briefings, Classification, and Visit/Meetings. Businesses safeguarding classified material on site will have an additional 152 questions/ inspection points. The safeguarding section has 18 main categories: "Marking Requirements; General Safeguarding; Standards for Security EQIPment; Storage; Intrusion Detection System; Information Control; Transmission of Classified Information; Destruction; Disclosure; Disposition; Retention; Termination of Security Agreements; Safeguarding; Subcontracting; Information Systems Security; International Security Requirements; Critical Nuclear Weapon Design Information; and COMSEC" (DCSA, 2020a). DCSA inspectors will score and provide feedback to the businesses if

they are deficient in an area. DCSA inspectors will also offer ways to implement changes to strengthen or fix deficiencies. If a company fails an inspection, it will be given time to correct the issues before reinspecting (DCSA, 2022). Once complete, the company will be granted its FCL.

THIS PAGE INTENTIONALLY LEFT BLANK

SUPPLEMENTALS

To access the supplemental materials listed here, contact the Dudley Knox Library or, for publicly releasable theses and supplementals only, visit the thesis pages in the library's Calhoun database.

A. SUPPLEMENTAL 1: FCL PROCESS MAP

Supplemental 1 FCL Process Map is a user journey depicting the FCL process and its supporting processes "as is" by the current instruction.

B. SUPPLEMENTAL 2: FCL PROCESS MAP AFTER RECOMMENDED CHANGES

Supplemental 2 FCL Process Map After Recommended Changes is a user journey depicting the FCL process and its supporting processes after applying the process recommendations of this capstone.

C. SUPPLEMENTAL 3: PROCESS MAP AFTER "TurboFCL" APPLICATION

Supplemental 3 FCL Process Map After "TurboFCL" Application is a user journey depicting the FCL process and its supporting processes streamlined by the "TurboFCL" application.

D. SUPPLEMENTAL 4: "TurboFCL" APPLICATION WIREFRAME

Supplemental 4 "TurboFCL" Application Wireframe is the framework for a phone application envisioned to streamline the FCL application process.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

ABSI Aerospace & Defense. (n.d.). *About*. Retrieved September 1, 2023, from https://absidefense.com/about/

Anduril. (n.d.). *Our Business*. Retrieved September 1, 2023, from https://www.anduril.com/mission/

APEX Accelerators. (n.d.). *What We Do*. Retrieved September 1, 2023, from https://www.apexaccelerators.us/#/about-us

Brown, J. (2023, July 17). DIU NPS Industrial Security Capstone Review. (B. Bushong, Interviewer) DCSA.

Clinton, W. (1996, February 5). *Executive Order 12988.* Government Publishing Office. https://www.gpo.gov/fdsys/pkg/FR-1996-02-07/pdf/96-2755.pdf

Collins Aerospace. (n.d.). *About Us*. Retrieved September 1, 2023, from https://www.collinsaerospace.com/who-we-are/about-us

DCSA. (2014). *National Industrial Security Program (NISP) Central Access Information Security System (NCAISS)*. DCSA. https://ncaiss-ps3.dss.mil/dss-cac-login/cert/login

DCSA. (2020a, February 26). *Submitting a Sponsorship Request External.* SAM. https://www.dcsa.mil/Portals/128/Documents/CTP/FC/Submitting_a_Sponsorship_request_External.pdf

DCSA. (2020b, February 6). *Request NISS Account External.* DCSA. https://www.dcsa.mil/Portals/128/Documents/IS/Request_NISS_Account_External.pdf

DCSA. (2021, March 09). *Facility Clearance (FCL) Orientation Handbook.* DCSA. https://www.dcsa.mil/Portals/91/Documents/CTP/FC/FCL_Orientation_Handbook_9_March_2021.pdf

DCSA. (2022). *NISP Tools & Resources*. Retrieved August 8, 2023, from https://www.dcsa.mil/Industrial-Security/National-Industrial-Security-Program-Oversight/NISP-Tools-Resources/

DCSA. (2023a, November 2). *Appeal an Investigation Decision*. Defense Counterintelligence. https://www.dcsa.mil/Personnel-Security/Background-Investigations-for-Applicants/Appeal-an-Investigation-Decision/

DCSA. (2023b). *Curricula*. Retrieved August 8, 2023, from https://www.cdse.edu/Training/Curricula/

Defense Acquisition Regulations System. (n.d.). *Federal Acquisition Regulation Part 32: Contract Financing*. Retrieved October 10, 2023, from https://www.acquisition.gov/far/part-32

Defense Advanced Research Projects Agency. (n.d.). *Bringing Classified Innovation to Defense and Government Systems*. Retrieved September 1, 2023, from https://www.darpa.mil/work-with-us/bringing-classified-innovation-to-defense-and-government-systems

Defense Counterintelligence Security Agency. (n.d.). *Mission, Vision, Values*. Retrieved September 1, 2023, from https://www.dcsa.mil/about-us/mission-vision-values/

Defense Information Systems Agency. (n.d.). *About DISA*. Retrieved September 1, 2023, from https://www.disa.mil/about

Defense Innovation Unit. (n.d). *About*. Retrieved September 1, 2023, from https://www.diu.mil/about

Defense Security Service. (2016). National Industrial Security Program Operating Manual. Washington, D.C.: Department of Defense.

DISA. (2023, October 8). *External Certification Authorities (ECA) – DoD Cyber Exchange*. Retrieved from Public.cyber.mil: https://public.cyber.mil/eca/

DSS. (2014, February). *E-QIP Signature Page and Electronic Fingerprint Guide For In-Process Facilities.* Retrieved from DCSA.mil: https://www.dcsa.mil/Portals/128/Documents/CTP/fc/eQIP%20Signature%20Page%20and%20Electronic%20Fingerprint%20Guide%20for%20In-Process%20Faci.pdf?ver=2snj-8ZvJwD5YYxXth3KOg%3d%3d

FSO PROS. (n.d.). *About*. Retrieved September 1, 2023, from https://www.fsopros.com/about.html

Glassdoor. (n.d.). *How Much Does A Facility Security Officer Make?* Retrieved October 10, 2023, from https://www.glassdoor.com/Salaries/facility-security-officer-salary-SRCH_KO0,25.htm

Hermeus. (2023, August 3). *We Are Hermeus*. Retrieved September 1, 2023, from https://www.hermeus.com/about

IdenTrust. (2022, October 21). *DoD ECA Programs*. Retrieved from IdenTrust: https://www.identrust.com/digital-certificates/dod-eca-programs

Jozsa, E. (2023). *National Office Report.* Vancouver: Commercial Edge.

Lofgren, E., & al., (2023, April 12). *Atlantic Council Commission on Defense Innovation Adoption interim report.* Retrieved from Atlantic Council Commission: https://www.atlanticcouncil.org/in-depth-research-reports/report/atlantic-council-commission-on-defense-innovation-adoption-interim-report/#conclusions

Mehls, M. (n.d.). *Company Details*. Retrieved September 1, 2023, from https://wiseengineeringconsulting.com/new-page-2

National Security Innovation Network. (n.d). *About Us*. Retrieved September 1, 2023, from https://www.nsin.mil/

Nooks. (2023, October 19). *About*. Retrieved September 1, 2023, from https://nooks.works/about/

Obama, B. (2011, January 18). *Executive Order 13563.* Government Publishing Office: https://www.govinfo.gov/content/pkg/FR-2011-01-21/pdf/2011-1385.pdf

Office of Small Business. (2023, October 8). *Home*. Office of Small Business: https://business.defense.gov/

Office of Small Business Programs. (n.d.). *Mission*. Retrieved September 1, 2023, from https://business.defense.gov/About/Mission/

OFFICE OF THE SECRETARY OF DEFENSE. (2022, July 1). *PART 117 – NATIONAL INDUSTRIAL SECURITY PROGRAM OPERATING MANUAL (NISPOM).* GovInfo. https://www.govinfo.gov/content/pkg/CFR-2022-title32-vol1/xml/CFR-2022-title32-vol1-part117.xml

PlainLanguage.gov. (2011, May 01). *Federal Plain Language Guidelines.* PlainLanguage. https://www.plainlanguage.gov/media/FederalPLGuidelines.pdf

Radical Firearms. (n.d.). *About Us*. Retrieved September 1, 2023, from https://www.radicalfirearms.com/aboutus.asp

Ries, E. (2011). *The Lean Startup.* New York: Crown Publishing.

Rollins, K. (2002, August 9). *Entity Validation.* SAM. https://www.gsa.gov/system/files/Stakeholder_Forum_-_Validation_-_August_9%2C_2022.pdf

U. S. General Services Administration. (n.d.). *Entity Registration Checklist.* Retrieved July 14, 2023, from https://iae-prd-videos.s3.amazonaws.com/pdf/entity-checklist.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Date=20231103T031233Z&X-Amz-SignedHeaders=host&X-Amz-

Expires=86399&X-Amz-Credential=AKIAY3LPYEEX2QGT3A5E%2F20231103%2Fus-east-1%2Fs3%2Faws4_request&X-

Verbout, J. (2021). *Access Ready Kiosk (ARK) White Paper.* Retrieved September 1, 2023, from http://www.scifinc.com/

WidePoint. (2023, October 8). *ECA Medium Assurance, ECA Medium Token Assurance, ECA Medium Hardware Assuarance Requests*. Retrieved July 21, 2023, from https://eca.orc.com/client-certificates/

Acquisition Research Program
Naval Postgraduate School
555 Dyer Road, Ingersoll Hall
Monterey, CA 93943

www.acquisitionresearch.net