Lessons for Defense Innovation from the Financial Cybersecurity Sector

Client Organization
United States Department of Defense
Defense Innovation Unit
National Security Innovation Network

Team Members
Ryan Henderson, Johann Kerhousse, Wes Lam, Sarah Quirk, Peter Zheng

Faculty Advisor
Elad Yoran

Date: May 2020

Table of Contents

Executive Summary

The financial services industry and its engagement with cybersecurity startups offers key insights into how the Department of Defense (DoD), including the National Security Innovation Network (NSIN), can bolster its own engagement with this startup community. As the DoD continues to pursue the development and implementation of next-generation information technology solutions, several current practices by the financial sector are applicable to the DoD and provide practical guidance for improving its engagement strategy.

Our report analyzed the practices of Globally Systemic Important Banks (GSIBs) and other large financial institutions to best gauge the financial services industry's current practices for working with cybersecurity startups. After eight interviews with key sector representatives, we believe these entities are the most comparable to the Department of Defense given their size and similarity in magnitude of cybersecurity threats faced.

We also analyzed the cybersecurity startup community's relationship with both the financial services industry and the DoD through nine interviews with industry leaders. Their range of professional experiences across the public and private sector highlighted key differences between the Department of Defense and financial services' interactions with startups as well as potential best practices to be shared. Our report discusses current DoD regulatory requirements and barriers to entry affecting engagement with the cybersecurity community, including security certifications and a recently-created contract bidding site.

Given the unique constraints and challenges faced by the DoD in partnering with cybersecurity startups, our team makes several recommendations to the Department of Defense and National Security Innovation Network for improving their engagement strategy:

1. **Increase the Department of Defense's visibility with enhanced commercial outreach and marketing, in particular at trade shows and startup fairs.** This could be accomplished with greater investment in marketing and committing more representatives from different DoD organizations to attend these events.
2. **Expand the Department of Defense's public-private partnership using Maryland's Defense Cybersecurity Assistance Program as a starting model.** The state's approach provides effective public-private partnership opportunities that reduce the knowledge and networking gap for startups interested in federal contracting.
3. **The Department of Defense Office of the Under Secretary of Defense for Research and Engineering, and possibly NSIN, could create and publish support material explaining all available pipelines for cyber startups to work with their network and the DoD at large.** Infographics highlighting "defense opportunities" for these startups and ensuring this document has significant viewership in search engines may pave the way for previously untapped engagement with small cybersecurity firms.

These proposals summarize our report's endorsement of more defense-focused professional events and networking, streamlined partnership processes with different funding programs, dynamic public relations campaigns and dissemination of clearer points-of-contact information.

Introduction

The fast pace of information technology modernization has become a top national security concern and defense priority for the United States. Historically, the U.S. Department of Defense has been at the forefront of information technology advancements, including the creation of the "internet" concept and its integration into a military communication intra-network called the ARPANET in 1969. Since then, the DoD has continued to pursue the development and deployment of next-generation information technology innovations in the modern-era of globally interconnected "cyberspace" – an all-encompassing term to include hardware and software products and operational tactics and techniques. With the globalization of the cyberspace industry, security has become a top priority to ensure the acquired technology is secure for use within various DoD systems. In recent decades, the increase in the number of cybersecurity incidents contributed to the creation of additional layers of product and operations certification requirements in the defense procurement process, such as hardware and software accreditations and personnel background and supply chain security investigations.

The goal of this capstone project is to identify lessons the DoD could draw from the financial sector's interactions with cybersecurity startups to obtain effective cybersecurity solutions. Our main objectives were to identify current practices within the financial sector for engaging with cybersecurity startups, assess the impact of these practices on the ability of the financial sector to transition new cybersecurity capabilities into their operations, and assess applicability of these practices to DoD's engagement with cybersecurity startups.

The project accomplished this task by performing three analyses. First, the project analyzed the financial services industry approach to researching, engaging, and investing in cybersecurity companies and adopting their technologies. The second set of analysis focused on experiences of cybersecurity firms' business partnership experiences with both defense and financial industries and gleaned from resulting data the common causes of partnership failures. Finally, we analyzed the current defense acquisition and procurement environment with an overview of authorizing environment, accreditation requirements, and defense contracting culture in order to identify potential barriers to entry for cybersecurity startups. The resulting assessment incorporated common threads from the three intersecting analyses and extrapolated from them recommendations offered at the end of the report.

Research Methodology

Types of Financial Services Industry Organizations Examined

In order to identify current practices within the financial sector for engaging with cybersecurity startups, we analyzed practices of Globally Systemic Important Banks and other large financial institutions. GSIBs are determined based on size, interconnectedness, lack of readily available substitutes or financial institution infrastructure, global activity and complexity.[1] They are critical infrastructure and highly regulated by the U.S. Government (USG). These organizations typically employ between 50,000 to 200,000 employees, are susceptible to cyber-attacks by both nation states and nonstate actors, and have the ability to buy or build necessary cybersecurity services. We believe that they are the private sector entity most similar to the USG, specifically the DoD based on this criterion.

In 2013, the USG released an Executive Order (E.O. 13636) "Improving Critical Infrastructure Cybersecurity". Critical infrastructures are designated by the USG as "those physical and cyber-based systems essential to the minimum operations of the economy and government" (Critical Infrastructure Protection PDD63). In Section 9 of Executive Order (EO) 13636, the government designates a series of companies "where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security".[2] In 2016, the Chief Executive Officers of eight GSIBs - Bank of America, BNY Mellon, Citigroup, Goldman Sachs, JPMorgan Chase, Morgan Stanley, State Street, and Wells Fargo - created the Financial Systemic Analysis and Resilience Center (FSARC) to "improve the resilience of critical functions that underpin the U.S. financial sector and to develop intelligence to protect and defend them".[3] We had the opportunity to speak to representatives from four of the eight members of FSARC, in addition to representatives from other GSIBs and large financial institutions.

A former CISO to a GSIB argues that the private sector, specifically the financial services industry, has better technology and more opportunities to combat cybersecurity on the front lines than the Federal Government. The financial services industry's cybersecurity risk is regulated by the Federal Government and employs many of the cybersecurity risk frameworks used by the government such as the National Institute of Standards and Technology's (NIST) framework for Improving Critical Infrastructure Cybersecurity. As cyber threats evolve, the Federal Government and financial services industry are continuously working to improve cybersecurity

[1] 'Global Systemically Important Banks: Updated Assessment Methodology and the Higher Loss Absorbency Requirement', 2013 <https://www.bis.org/publ/bcbs255.htm> .
[2] 'Executive Order -- Improving Critical Infrastructure Cybersecurity', *Whitehouse.Gov*, 2013 <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity> .
[3] 'FSARC_TMPG_Presentation.Pdf' <https://www.newyorkfed.org/medialibrary/Microsites/tmpg/files/FSARC_TMPG_Presentation.pdf> .

defenses and mitigate cyber risk using a wide range of tools and services. Each industry must make a decision on whether to build or purchase a cybersecurity service and uses a different methodology to make these determinations. The goal of our research is to identify best practices of FSI organizations' engagement with cybersecurity startups and assess the impact of these practices on the ability of the financial sector to transition new cybersecurity capabilities into their operations.

Types of Startups Examined

To develop a clear picture of the cybersecurity startup landscape, we interviewed nine industry leaders with a variety of experience across public and private sectors. This ranges from a director responsible for technical advisory services in the insurance market and CEOs of early-stage Venture Capital (VC) firms to former Chief Security Scientists and Sales Directors. Over half of the interviewees had previously provided services to the DoD and FSI, while all individuals had partnered with at least one.

For the purposes of the report, we defined cybersecurity startups as having less than 100 customers, $25 million in revenue, less than 200 employees and $50 million in capital. One interviewee suggested these were "aggressive" estimates and that there should be less focus on revenue and number of customers since the size of each customer plays a considerable role. In multiple interviews, the number of years in operation was described as critical to determining if a company should still be labeled as a true startup. One individual running an early-stage VC suggested cybersecurity companies under seven years of operation could be deemed startups.

Our goal was to interview startup leaders who have addressed these obstacles with various strategies created through their own ventures, as well as best practices they suggest for bolstering the DoD-cyber startup relationship. Several interviewees recognized that the government has improved its commitment to startup partnerships, including through Defense Innovation Unit (DIU), but also said startups still "have no structural way to differentiate themselves from one another". These barriers to entry and potential solutions identified by our interviewees will be examined in further detail in the following sections.

DoD Regulatory Requirements

To better understand the environment and culture of defense acquisition, one must first recognize authorities under which the DoD operates and imposes security requirements, especially for systems of different classified levels and compartments. In order to focus on one specific system domain with simpler accreditation requirements, we analyzed contract projects for the unclassified domain within the DoD. Executive Order 13556 "Controlled Unclassified Information" was established in November 2010 as a way of standardizing the government-wide

processes for handling Controlled Unclassified Information in the various USG systems.[4] While E.O. 13556 outlines the purpose and goal of information handling requirements and processes, NIST special publication 800-171 "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations" (Revision 2; February 2020) provides detailed requirements for processing of Controlled Unclassified Information on non-government (or "nonfederal") systems. This includes financial transactions, e-mails, security clearances, healthcare records, various cloud services, and defense research and development.[5]

NIST 800-171 is one of the basic security certifications that cybersecurity startups must adhere to in order to work with the DoD. This process, the first barrier to entry, is done through a series of defense-specific regulations called the "Defense Federal Acquisition Regulation Supplement" (DFARS).[6] As a whole, these regulations address two essential goals – fostering adequate security and rapid cyber incident reporting.[7]

The second barrier to entry are the investigations required of the firm, its personnel and its supply chain. The investigative agency within the DoD that conducts Personnel and Facility Security Clearance-related processes for all security clearance levels, such as background investigations and adjudications, is the Defense Counterintelligence and Security Agency (DCSA). After the Office of Personnel Management (OPM) Cybersecurity Incident of 2015, the duty of federal and contractor background investigations was transferred from OPM's National

[4] EO 13556 excludes the handling of classified and sensitive information procedures that are detailed in a series of other Executive Orders such as EO 13526 "Classified National Security Information" – Top Secret, Secret, and Confidential – and the Atomic Energy Act, where each of the classified systems has its own requirements. For more information on EO 13556, please see '3 CFR 13556 - Executive Order 13556 of November 4, 2010.' *U.S. Government Publishing Office (GPO).* <https://www.govinfo.gov/app/details/CFR-2011-title3-vol1/CFR-2011-title3-vol1-eo13556> ; for more information on Classified Information-related requirements, please see EO 13526 referenced in the report, EO 12829 "National Industrial Security Program", EO 13549 "Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities", and EO 13587 "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information"; for more information on The Atomic Energy Act, please see 'Atomic Energy Act of 1954.' *Office of the Legislative Counsel - US House of Representatives.* <https://legcounsel.house.gov/Comps/Atomic%20Energy%20Act%20Of%201954.pdf>

[5] According to the NIST: "A federal information system is a system that is used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency. A system that does not meet such criteria is a nonfederal system." For more information on NIST 800-171, please see 'NIST Special Publication 800-171' *US Department of Commerce - National Institute of Standards and Technology*. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf>

[6] The defense information security-related regulations can be found in DFARS 252.204—7000 "Disclosure of Information," –7008 "Compliance with Safeguarding Covered Defense Information Controls," –7012 "Safeguarding Covered Defense Information and Cyber Incident Reporting," –7014 and –7015 provide guidelines on the disclosure of litigation related information, and –7016 to –7018 provide guidelines on "Covered Defense Telecommunications Equipment or Services". For more information on the DFARS regulations referenced in the report, please see 'DFARS; Revised April 8, 2020' *Office of the Under Secretary of Defense for Acquisition & Sustainment.* <https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm>

[7] Expert defense contractors who can perform self-assessment by using the NIST SP 800-171 Self-Assessment Handbook, or alternatively, firms can hire Managed Security Service Providers (MSSP) who specialize in Defense Contracting and DFARS requirements. For more information on the NIST 800-171 Self-Assessment process, please see 'NIST Handbook 162: NIST MEP Cybersecurity Self-Assessment Handbook' *US Department of Commerce - National Institute of Standards and Technology*. <https://nvlpubs.nist.gov/nistpubs/hb/2017/NIST.HB.162.pdf> ; for more information on an example of DFARS MSSP, please see firms such as SysArc https://www.sysarc.com/services/managed-security-services/dfars-compliance/

Background Investigation Bureau (NBIB) to DCSA in October 2019.[8] For general unclassified systems, the DCSA is designated by the Under Secretary of Defense for Intelligence (USDI) to perform as the DoD Enterprise Management of Controlled Unclassified Information.[9] For defense contractors, the security vetting process varies depending on the level and type of security clearance and the number of applications in each of the security queues.

Anecdotal evidence showed that application processing takes approximately 100 days, investigation takes approximately 290 days, and adjudication takes approximately 45 days depending on the sponsoring agency's office. The estimated 435 days of overall clearance processing can simultaneously include DFARS and NIST compliance certifications. The more than one year of clearance processing is far too long for most startups, whose operating cycle might not have the capital to wait for the sales decision of a product or service contract from DoD. Additionally, the high opportunity cost associated with an overly lengthy process is in stark contrast with the comparatively shorter approval process of a private sector firm. Even if the DoD reduces its overall processing time by 50%, the resulting seven months would still take up most of the startup's fiscal or financial year resulting in high opportunity cost.

Landscape Assessment

Current DoD Contracting Environment and Additional Barriers to Entry

Prior to 2020, there was not a comprehensive defense contract bidding process site. The information was scattered across different websites for various government offices. However, the General Services Administration (GSA) has started its service centralization process by merging different offices and functions into a centralized portal called System for Award Management (SAM). During the first quarter of fiscal year 2020, the GSA began the migration from the Federal Business Opportunities (FBO) portal to the "betaSAM" portal.[10] The betaSAM portal

[8] For more information on the OPM Cybersecurity Incident of 2015, please see 'Cybersecurity Resource Center: Cybersecurity Incidents.' U.S. Office of Personnel Management (OPM). <https://www.opm.gov/cybersecurity/cybersecurity-incidents/> ; for more information on EO 13869 "Transferring of Responsibility for Background Investigations to the Department of Defense", please see 'DCPD-201900238 - Executive Order 13869-Transferring Responsibility for Background Investigations to the DoD' *U.S. Government Publishing Office (GPO)* <https://www.govinfo.gov/app/details/DCPD-201900238>

[9] A Senior Action Officer Working Group is established in 2018 that included the following officers: USDI, DoD Chief Information Officer (CIO), DoD Office of Secretary of Defense (OSD) Acquisitions and Sustainment (A&S), DoD OSD Research and Engineering (R&E), DoD Missile Defense Agency (MDA), DoD Defense Contract Management Agency (DCMA), (National Archives and Records Administration – NARA) Information Security Oversight Office (ISOO), and Services. For more information on the DCSA and its missions, please see 'DCSA-Critical Technology Protection: Controlled Unclassified Information' *Defense Counterintelligence and Security Agency.* <https://www.dcsa.mil/mc/ctp/cui/>

[10] 'Contract Opportunities' *U.S. General Services Administration (GSA)-Integrated Award Environment (IAE).* <https://www.gsa.gov/about-us/organization/federal-acquisition-service/office-of-systems-management/integrated-award-environment-iae/betasamgov-information-kit/contract-opportunities-formerly-federal-business-opportunities> ; 'FBO is Transitioning to Beta Factsheet' *U.S. General Services Administration (GSA)-Integrated Award Environment (IAE)* <https://www.gsa.gov/cdnstatic/FBO_Is_Transitioning_to_Beta_Factsheet_%281%29.pdf>

contains all federal contracts and their respective agencies and sub-agencies. In order to do business with the USG, contractors and vendors are required to register on the SAM portal.[11]

Another obstacle that new defense companies might encounter includes the numerous large defense firms such as Lockheed Martin and Booz Allen Hamilton. Some of these firms have over 50 years of government service experience as prime contract holders, also known as "primes". Unofficially, these primes operate collectively as "Defense Cartels" and often act as gatekeepers for various government agencies and sub-agencies through their decades of relationship building, professional networking, and successive contract holdings, the last of which creates an unofficial barrier for new defense startups to enter into the bidding process. In service sectors like Computer Network Operations (CNO), this industry culture makes it difficult for new defense companies to enter the market, where the lowest bid is often artificially capped via various nondisclosed industry mechanisms.[12]

However, in the 1990s certain policy measures were implemented to facilitate change and to encourage small businesses to enter into DoD, and federal contracts in general, via the Best Value method instead of Lowest Bidder method. Policies known collectively as the Clinger-Cohen Act enabled small and startup companies to bid on government purchases up to $100,000 through the Best Value method. Another popular strategy for startups and small businesses is to operate as a subprime or subcontractor as their first venture into the defense market. This shifts the majority of the overhead cost to the primes while allowing new defense companies to focus on providing their product and service to the government client, thus building up industry reputation and capital.[13]

Impact of COVID-19 on Cybersecurity Startups

COVID-19 has negatively impacted VC funding for new startups. Some 43 venture capital deals have closed as of mid-March this year, compared to 103 deals in the first two months of 2018

[11] The betaSAM portal's DoD search returned with its 39 sub-tier agencies and the most recent cybersecurity contract dated April 7th, 2020 supporting the U.S. Air Force's Enterprise Data Loss Prevention (E-DLP). For more information on the betaSAM portal and to access the federal contract service, please see https://beta.sam.gov/search?keywords=All%20Defense%20contracts&sort=-modifiedDate&index=&is_active=true&page=1; for more information on the USG vendor registration process, please see https://www.sam.gov/SAM/

[12] Information on certain defense industry firms' insider practices that may include non-compete mechanisms are anecdotal. Since NDAs are signed by former employees upon departure, specific business practices are not described.

[13] For more information on Federal Acquisition Streamlining Act of 1994 and case decision, please see 'The FASA of 1994 - Fair opportunity procedures under multiple award task order contracts.' *U.S. Government Accountability Office (GAO).* <https://www.gao.gov/decisions/other/302499.pdf> ; for more information on FARA, please see 'Federal Acquisition Reform Act' *U.S. Department of Commerce - Office of Acquisition Management.* <https://www.osec.doc.gov/oam/archive/docs/FARA.pdf> ; for more information on ITMRA and Clinger-Cohen Act, please see 'DoD Chief Information Officer Desk Reference: Volume I Foundation Documents' *U.S. DoD: Office of Small Business Programs.* <https://business.defense.gov/Portals/57/Documents/Federal%20Acquisition%20Reform%20Act%20of%201996%20Clinger-Cohen%20Act.pdf>

and 91 deals over the same period in 2019.[14] Many VC firms and investors are injecting more liquidity and cash into well-established series B, C, D+ ventures in hopes that the companies will ride out the 2020 economic hardships. They believe that startups in this funding round will have a higher likelihood of surviving the economic hardship whereas earlier stage companies have a greater likelihood of failing.

For cybersecurity startups, the current environment will adversely affect access to funding and has led many companies to lay off or furlough employees. The consensus is that there will be overall fewer investments into cybersecurity startups, but greater funding to those that are well-established, as the abrupt shift to remote working due to coronavirus concerns has fostered an environment ripe for cybersecurity as many firms face unprecedented cyber threats. For example, Zoom, an online meeting tool, has been under intense scrutiny from government officials and users. Complaints about security and privacy of meetings, including hackers intermittently joining these calls, dominated media attention as the world gravitated towards the platform for school and work. This resulted in Zoom hiring Alex Stamos, ex-Facebook security boss. The company is not alone, as many other platforms like Google Hangouts and Microsoft Teams have announced an increase in cyber-attacks since work from home began. However, these firms are more established and have the online infrastructure and resources to curtail security threats. Regardless of fewer investments during this pandemic, cybersecurity remains critical to governments, businesses and consumers. Investors will continue to fund promising companies even if the process is elongated.

Current Practices for the Private Sector

How Financial Services Industry Engage Cybersecurity Startups

In our research and interviews with representatives from GSIBs and other FSI organizations, we were able to determine key factors in how the FSI engages with cybersecurity startups. First, many organizations have a designated team for identifying cybersecurity startups. Second, there are two ways these teams identify startups – formally through technology conferences and informally through networking amongst peers. Third, cybersecurity startup identification begins with a specific requirement needing to be addressed, general area of interest for the medium-long term interest for the firm, and/or identifying a good investment opportunity.

Many FSI executives agreed that cybersecurity startups are defined by the amount of capital they have raised. A CISO to a GSIB noted that startups can be defined differently depending on the industry. This means a company that has investment and product deployment in the public sector may not be considered a startup by the USG, but could be classified as a startup by the private

[14] Stone, Jeff. "Venture Funding in Security Startups Is Falling. Don't Blame the Coronavirus." *CyberScoop*, 19 Mar. 2020, www.cyberscoop.com/cybersecurity-venture-capital-2020-funding-datatribe/.

sector. When banks are identifying startups, they are looking at many characteristics that range from sustainability using a risk perspective to scalability using a technology perspective. The evaluation of the sustainability of the startup can include a review of their investors, leadership track record, business plan, handling of confidential data, etc. Teams evaluate the scalability of a product by taking the product and simulating it in the product environment using labs. FSI executives shared that it is during this stage that much of the technology doesn't scale.

Many FSI organizations have dedicated teams to identify technology needs for the firm and where to find them when the need cannot be addressed internally or by a current third-party vendor. These teams are actively engaging with the cybersecurity startup community through technology conferences and mentorship programs, even when there is not a specific cybersecurity need for the FSI organization. Banks also have groups that identify cybersecurity companies in which the bank should consider investing. According to a CBInsights report, "in 2018, firms such as J.P. Morgan Chase & Co., Citigroup, Barclays, Goldman Sachs, and others participated in 13 deals to cybersecurity startups — a record high for banks investing across the cybersecurity space".[15] This allows a bank to find or build a solution for a technology issue in addition to capturing financial benefits.

There are two main ways FSI organizations identify cybersecurity startups formally and informally. It is important to note that the financial services industry does not compete when it comes to cyber resilience. The industry is highly collaborative to help its members to mitigate cyber risks as a whole. The informal identification process of networking cybersecurity contacts amongst peers is indicative of this team mentality. In an interview with a CISO to a GSIB, the CISO said that, "if I've never heard of a startup then I am no more than one degree removed from someone who knows them - it's not that big of a community. If you're legit then you're no more than two degrees of separation from the CISO". Another financial services executive said that cybersecurity startups can be identified "internally using word of mouth from other people in the company".

Teams at these institutions that identify cybersecurity startups have a strong brand in the cybersecurity ecosystem which is developed by engaging with cybersecurity startups more formally. Many GSIBs host their own technology weeks and regularly send representatives to attend cybersecurity conferences such as RSA and Defcon. A former CTO to a GSIB said that during a technology conference in California,

> "they take a list of 2,000 startups and filter to 150 companies that they wanted to hear from. [They] divide teams into small groups and perform 'speed dating' [and] grade

[15] 'Banks Are Backing More Cybersecurity Startups Than Ever Before', *CB Insights Research*, 2019 <https://www.cbinsights.com/research/top-banks-cybersecurity-investments-expert-intelligence/>.

> startups on a 1 to 5 scale. If a startup was successful, they do a deep dive, invite them to the labs and deploy ‘a’ solution . Grading questions often included: how relevant is the technology to the firm; how mature is the technology; Is the technology relevant in the market”.

Institutions also develop partnerships with cybersecurity startups through innovation forums hosted by professional organizations that they are members of such as FS-ISAC where startups will pay to present in front of member organizations.

One industry expert says that the FSI targets a specific defined operational need and will often aim to mix building and buying to continue to engage with the community to stay informed. Certain organizations pride themselves on partnering with cybersecurity startups and further preparing them to operate in the financial services environment. From a business perspective, a GSIB may choose to invest in a startup to help design products and define requirements. This allows the organization to both find a solution to a specific cybersecurity need and gain a financial benefit.

How Cybersecurity Startups Engage the Financial Sector and DoD

Based on responses from interviews with leaders in the cybersecurity startup space, LinkedIn was a primary mechanism in contacting financial industry leaders. The FSI is more transparent with job titles and companies, resulting in easier access for startups to initiate a cold network. With an early stage cybersecurity, the team typically in charge of spearheading these relationships is the business development unit with representatives conducting cold calls and outreaches with the methods listed above.

Comparatively, many startups found it more difficult to maneuver within the DoD. Titles and departments of the individuals were not readily accessible, making it harder to initiate a cold network. One respondent said the DoD’s organizational chart is fluid and unclear while private sector organizational charts are well-defined. One could easily check the company webpage for the appropriate point of contact and facilitate an email introduction or a LinkedIn message. Another respondent classified the DoD identification process as “a scavenger hunt with sometimes no end in sight”, curtailing the effectiveness of professional networking platforms (LinkedIn) for accessing DoD officials.

In addition, our respondents highlighted cybersecurity conferences and trade-shows as important to fostering organic interactions between the client (DoD or FSI) and vendors (cybersecurity firms). These conversations can be set up in advance of the conference so individuals are aware of who they will be meeting or can exchange professional contact information to get their foot in the door.

Another important method mentioned by respondents were personal relationships and utilizing their professional network (work colleagues) to facilitate introductions to both the DoD and FSI. Cybersecurity startups can connect with the DoD representatives, who can then redirect them to other personnel if they are not the correct point of contact. Similar sentiments surfaced for the FSI, however interviewees noted it was useful having existing vendors that the banks worked with to facilitate the introduction.

Impact Assessment

Financial Services Industry's Operational Complexity: Centralized vs. Decentralized
Based on preliminary observations of the qualitative surveys performed within the FSI, we would like to explore further how the operational complexity of the firm appears to be linked to its ability to transition new cybersecurity capabilities quickly. For example, we observed that some larger organizations with a considerable footprint, such as those with a sizable physical retail business, tend to operate in a decentralized manner. While overall guidance and group level agreements will be directed by the head of information security, leaders across the bank's departments maintain authority over relevant cybersecurity practices as well as the budget and decision-making power that follow from it. An enterprise-level cybersecurity solution like anti-phishing technology will reside at the CISO level and require a CISO response. However, the cybersecurity solution that is unique to a business, like automated security intelligence for a specific business unit, will sit at the departmental level while the CISO team acts as an advisor with subject matter experts remaining in the lead role. We believe that this decentralized approach to decision making is also emulated in the Department of Defense procurement process, namely division level procurement decisions versus undersecretary level procurement decisions.

From the FSI perspective, our research indicated that increases in the number of stakeholders in operationally complex and decentralized firms further prolong the time required to deploy new cybersecurity solutions. On average, these firms take 12 to 18 months to move from scope-of-work phase to implementation. A protracted timeline allows the large decentralized player to perform a thorough diligence process, particularly in testing for scalability in the technology. Given the relationship-based nature of the cybersecurity space, this type of financial firm will rely more heavily on formal and informal "word of mouth" mechanisms (such as through industry group FS-ISAC or peers) to identify relevant startups and technologies.

In contrast, specialized financial firms with a limited footprint, especially investment banks, tend to operate their cybersecurity services in a centralized manner. Overall guidance, group level agreements, budgets and decision-making power resides with the CISO. Whether the cybersecurity solution is unique to a business unit or a strategic enterprise value, the CISO's core

team of direct reports remains the main accountability body. Based on our qualitative survey, increased centralization of cybersecurity specific processes tends to increase the level of strategic partnerships existing between firm and startup.

Agility and swiftness best describe the centralized firm's ability to transition new cybersecurity capabilities into their operations. Centralization allows for better understanding of the cybersecurity needs of the bank, as well as implementation of more coherent cyber risk mitigation strategies. On average, these firms take three weeks to six months to progress from scope-of-work phase to deployment. Because these firms can be reactionary, the procurement depends on the need which allows them to accelerate the traditional due diligence. While some firms operating in a cyber-decentralized manner grant cyber startups access to internal mentorship programs, the cyber-centralized financial firm tends to be more actively engaged in the financial success of the startup. Usually taking the form of sizable investment positions, some cyber-centralized firms recommend startups for acquisition to dominant players in the technology industry, such as Microsoft. These practices tend to increase the effectiveness of financial firms to operationalize acquired cyber technology.

Challenges Faced by Cybersecurity Startups

The DoD's approach for engaging startups faces a series of problems. First, many interviewees pointed to the difference in engagement models for the FSI and the DoD. While the FSI often begins its relationship with startups through warranted introductions between a bank advisor and startup company representative, the DoD operates through federal contracts. Navigating the contract process is unfamiliar for most startups, who often face the decision of hiring a seasoned and expensive professional with experience in dealing with government clients. Startups functioning as technology services vendors often lack the cash and time to hire advisers to maneuver the procurement process, which can cost between $250,000 and $1 million.[16] Moreover, the process requires a two-year commitment before meaningful revenues can be expected. This is a considerable financial risk and prohibitive to many startups, which revert to working under established government contractors if hiring an adviser is not feasible.

A key challenge for product sellers is gaining government safety certifications. Senior Department of Defense officials have emphasized the importance of protecting the Defense Industrial Base (DIB) from a growing number of cybersecurity threats. The DoD helped address this concern by releasing Version 1.0 of the Cybersecurity Maturity Model Certification (CMMC) in January 2020. This model is a "marked departure from prior DoD cybersecurity compliance mandates" by requiring each of the estimated 300,000 contractors and subcontractors

[16] Syeed, Nafeesa. "Tech Startups Struggle to Tap $82 Billion in Federal Contracts." *Bloomberg*, 8 Dec. 2016, www.bloomberg.com/news/articles/2016-12-08/tech-startups-struggle-to-tap-82-billion-in-federal-contracts.

in the DIB to reach a cybersecurity certification through a third party by 2026.[17] Contractors will face heightened scrutiny of procedures used for controlling access, employee training, incident response, securing information and assessing risk of intrusions. The Department of Defense said the CMMC is a "flexible blueprint for effective cybersecurity" and will not impose significant additional compliance or audit costs on smaller contractors or subcontractors.[18] However, there is uncertainty about whether the CMMC will deter commercial companies and startups from participating in future DoD contracts. As of March 2020, the DoD has yet to provide details on the certification timeline, announce procedures for contesting certification determinations or identify a practical way to certify 300,000 companies in less than six years.

One potential issue is the impact on suppliers operating further down the supply chain. If the Defense Department requires "downstream suppliers to achieve the same CMMC certification as the prime contractor, that could significantly increase the cost of critical components and drive away smaller suppliers", particularly those lacking a robust compliance function.[19] Startups which need to bolster their cybersecurity in response to CMMC will inevitably need the assistance of specialists to provide the necessary equipment, software and procedures. Ellen Lord, Undersecretary of Defense for Acquisition and Sustainment, said that the DoD and Small Business Administration will provide assistance to startups where possible.[20] The Department of Defense also announced that cybersecurity costs will be an "allowable cost" under DoD contracts, which would offer small companies a chance to recover some of the associated compliance costs.[21] However, the bottom line is that even if a startup has rigorous cybersecurity protections already in place, it may still have to bear the costs of undergoing an audit and receiving a CMMC certification.[22]

In recent years, the DoD's service branches have worked to overcome bureaucratic hurdles and expand relationships with smaller tech-focused companies. The Air Force's use of Other Transaction Authority (OTA) as alternative transaction agreements to cumbersome DoD acquisition processes enables small and nontraditional defense firms with little to no experience or understanding of contracting with DoD to obtain an award much faster.[23] However, DoD's conventional long-term, large-scale procurement is still unattractive for many cybersecurity startups. Government clients frequently revert to buying through primes like Booz Allen

[17] "Recently-Released Cybersecurity Verification Mandate Creates Uncertainty for Department of Defense Suppliers." *The Trade Practitioner*, 7 Mar. 2020, www.tradepractitioner.com/2020/03/cybersecurity-verification-mandate-dod-suppliers/.
[18] Ibid.
[19] Sybert, Sarah. "Why Government Contractors Are Uncertain of DoD's CMMC Regulations." *ExecutiveGov*, 10 Mar. 2020, www.executivegov.com/2020/03/why-government-contactors-are-uncertain-of-dods-cmmc-regulations/.
[20] Goldstein, Phil. "What Comes Next for the DOD's Cybersecurity Certification Regime? ." FedTech, 9 Jan. 2020, fedtechmagazine.com/article/2020/01/what-comes-next-dods-cybersecurity-certification-regime.
[21] Schoonover, Matthew. "5 Things You Should Know: CMMC." *SmallGovCon*, 18 Feb. 2020, smallgovcon.com/five-things/cmmc/.
[22] Ibid.
[23] Ehlinger, Samantha. "Counter-Drone Tech, Multi-Factor Authentication Featured in DIUx's 13 New Agreements." *FedScoop*, 20 Apr. 2017, www.fedscoop.com/counter-drone-multi-factor-authentication-featured-diuxs-13-new-agreements/.

Hamilton or Accenture. This preference results in narrower options for the client because even if an established intermediary is able to find a solution through a smaller firm's service or product, the intermediary itself may not be aware of all viable startups for the client's needs. One interviewee called the DoD "a creature of habit" that still makes itself unavailable to startups with potential to bring solutions to them. The DoD continues to be "very cryptic" on how smaller companies can help them, and startups who haven't established a name for themselves in the industry, "[it] needs to have a recommendation provided by a previous vendor they engage with to even get [the DoD] to speak with you".[24]

While prime contractors have established channels for ongoing communication with government clients, cybersecurity startups lack the personnel to build or maintain these relationships. There are efforts on the federal side to close this gap. GSA's 18F office opened an office in San Francisco where startups can meet government officials. It is also experimenting with ways to "cut the red tape [by] 'micro-purchasing' particular goods…and quickly authorizing some small firms to do 'agile' tech projects".[25] However, this outreach effort has been limited in capacity and effectiveness. Several interviewees said the DoD lacked an open forum to discuss new and innovative ideas developed by smaller cybersecurity companies. Not having a clear audience or venue to present their services remains a noticeable deterrent within the startup community.

For many startups, selling to the government is an opportunity to establish themselves in the industry. Reputation and referrals carry significant weight in both the public and private sector, but startups may hesitate to focus on the federal side. While the federal government continues to be a large source of business for cybersecurity companies, there are growing opportunities in the commercial sector, which analysts estimate will reach $202 billion by next year. This expanding market is an attractive alternative for companies that "cut their technology teeth providing... services for the federal government, where spending has largely stagnated".[26] Enduring multi-year acquisition cycles may become a disincentive in the face of other opportunities in the commercial sector. Furthermore, federal contractors are often at the discretion of their client, which stifles the creativity present in many startups. While the commercial side may seem more navigable than government contracts, startups must still take into consideration that the product, pitch, size of the deal and business model are very different.[27]

Another challenge for startups developing new cyber technology is that the government often seeks niche solutions. The commercial world quickly generates new technologies, which means cybersecurity startups must continue to innovate to remain competitive. Meeting specific government needs is difficult because startups often cannot afford to specialize. If startups are

[24] Quote from an executive officer from Company C. [interviewed on 11 March 2020].
[25] Syeed, Nafeesa. "Tech Startups Struggle to Tap $82 Billion in Federal Contracts." *Bloomberg*
[26] Gantz, Sarah. "Going Commercial a Challenge for Government Contractors." *The Baltimore Sun*, 28 Apr. 2017, www.baltimoresun.com/business/bs-bz-commercial-cyber-challenge-20170425-story.html.
[27] Ibid.

geared towards developing solutions for government offices that are still far behind in implementing new products or services, they may put themselves at a competitive disadvantage for competing in the commercial cybersecurity market.

Moreover, there is a noticeable gap in technical expertise between the government and private sector, including the financial services industry. The FSI is much more equipped to evaluate the startup space because they have a more thorough understanding of the cybersecurity ecosystem. While banks have teams staffed with specialists in emerging technologies, the government has frequently filled these equivalent roles with project managers unfamiliar with the technology being presented by the startup community. The DoD has operated primarily as a consumer within the cyber industry and continues to lag in determining how to match newly arrived products or services with their niche requirements. Startups recognize that they can get higher value by going to the commercial market rather than the government. For a cash-strapped firm, this can be a major inhibitor to considering the DoD or other USG clients.

Lastly, proof of concept is a challenge for both the DoD and startups. For the Department of Defense, it is difficult to perform a proof of concept for a security capability because, by nature, the feature is previously unknown. The demonstration must be completed using a known issue or vulnerability. This presents a challenge in interpreting whether a startup's performance in a proof of concept will carry over to situations faced after the demonstration. Federal customers may be hesitant to make an investment in a technology whose performance was only shown in a narrow simulation. Proof of concepts are also expensive for the end user because they have to dedicate space, resources, staff and money. On the other hand, startups still need access to data to demonstrate and validate their product. Without defined requirements of criteria from the client, startups may not be able to communicate the full scope of their proposed solution.

Federal Government Funding and Assistance Programs for Cybersecurity Startups

Federal Programs such as the Small Business Innovation Research (SBIR) and the Small Business Technology Transfer Program (STTR) are two of the largest and most popular seed funding pools at the federal government level. At the DoD level, the SBIR and STTR funds are managed by the Office of the Under Secretary of Defense (OUSD) for Acquisition & Sustainment and applicants can submit proposals online through DoD's Defense SBIR/STTR Innovation Portal (DSIP). The portal includes opportunities from different Small Business program offices within the DoD, for example Defense Advanced Research Projects Agency Small Business Program Office (DARPA SBPO), Defense Information Systems Agency Office of Small Business Program (DISA OSBP) and DISA Technology Transfer Program (T2).

In 2018, DISA awarded $1.6 billion in prime contracts to small businesses. Currently there are over 6,500 contracts representing 28% of all contracts awarded by DISA. One policy tool that enables the private-public-partnership is the Cooperative Research and Development Agreement

(CRADA). Programs like T2 are authorized under CRADAs to foster relationships with private sector industry, universities, local and state governments, and other federal agencies and laboratories. Alternatively, projects funded by defense contractors independent of DoD control and financial support is the Defense Innovation Marketplace (DIM) Independent Research & Development (IR&D) program. This portal is hosted by Defense Technical Information Center (DTIC), whose mission is to connect the private industry with the defense industry.[28]

State Government programs are a popular starting point for many defense startups and small businesses that need preliminary guidance into the defense contracting industry. While certain states have offered business development assistance, the State of Maryland has an official federally funded, state-sponsored program that offers various funding and compliance assistance in order to attract new and existing cybersecurity businesses who are interested in venturing into the defense contracting industry.

One of the federal-state partnership's flagship programs is the Defense Cybersecurity Assistance Program (MD DCAP). The program is funded by DoD Office of Economic Adjustment (DoD OEA) through the MD Department of Commerce. It assists small businesses with DFARS and NIST 800-171 compliance and requirements. MD DCAP also provides over $10,000 for expenses during the compliance certification period such as remediation cost. In order to ensure continual success of Maryland's small businesses, the state also implemented a business portfolio diversification program called the MD Defense Diversification Assistance Program (MD MDDA), whose goal is to prepare MD defense businesses with 35% or more of annual revenue from the DoD for entry into new commercial domestic and international markets. Additionally, in order to facilitate in-state commerce, MD also implemented the Buy Maryland Cybersecurity (MD BMC) Tax Credit program, where products and services sold by qualified MD Cybersecurity Sellers can have up to $400,000 in annual tax credit.[29]

---

[28] DSIP also publishes other DoD subordinate organizations' Small Business Program projects, e.g. from DARPA Small Business Program Office; 'Defense SBIR/STTR Innovation Portal (DSIP) - Proposal Submissions' *U.S. DoD.* <https://www.dodsbirsttr.mil/submissions/login> ; 'Defense Innovation Marketplace (DIM)' *U.S. DoD Defense Technical Information Center (DTIC).* <https://defenseinnovationmarketplace.dtic.mil/business-opportunities/dod-agencies/> ; 'Public Law 99-502-OCT. 20, 1986: Technology Transfer Act of 1986' *U.S. Government Publishing Office (GPO).* <https://www.govinfo.gov/content/pkg/STATUTE-100/pdf/STATUTE-100-Pg1785.pdf> ; '(Title) 15 US Code § 3710a. Cooperative research and development agreement' *Cornell Law School: Legal Information Institute.* <https://www.law.cornell.edu/uscode/text/15/3710a> ; 'DISA Technology Transfer Program (T2)' *U.S. Defense Information Systems Agency.* <https://www.disa.mil/About/CTO/Technology_Transfer_Program>

[29] Maryland's Manufacturing Extension Partnership (MD MEP) is funded by the industry and the state to focus on strengthening local manufacturing. It specifically serves small- and mid-size firms with less than 500 employees and it is part of NIST's larger Manufacturing Extension Partnership (NIST MEP). 'MEP' *State of Maryland.* <http://www.mdmep.org/>; 'MD DCAP' *State of Maryland.* <http://www.mdmep.org/maryland-defense-cybersecurity-assistance-program/>; DoD's OEA manages partnership programs and distributes funds to state and local governments in support of defense requirements, please see 'Community Investment' *DoD Office of Economic Adjustment (OEA)* <https://www.oea.gov/our-programs/community-investment>; 'MD MDDA' *State of Maryland.* <https://commerce.maryland.gov/fund/programs-for-businesses/maryland-defense-diversification-assistance-program-(mdda)>; and 'MD BMC' *State of Maryland* <https://commerce.maryland.gov/fund/programs-for-businesses/buy-maryland-cybersecurity-tax-credit>

Recommendations and Summary

Our recommendations for the DoD on how to interact with the cyber startup community to obtain the most effective cybersecurity solutions are two pronged: DoD-level recommendations and those specific to NSIN.

Department of Defense

Our first recommendation is to have the DoD partner with trade shows or startup fairs and promote their own visibility at these events through greater marketing. For example, defense-related nonprofit sponsor events such as the Air Force Association's 2019 Air, Space, and Cyber Conference that was held at the National Harbor in Maryland, and the Armed Forces Communications and Electronics Association (AFCEA), which was established in 1949, has annual conferences and a Small Business Office to assist startups and small firms.[30] This method enables interested and potential cybersecurity startups to engage directly with DoD organizations who present their requirements and are actively searching for solutions. It also allows the cybersecurity ventures to be in contact with the appropriate DoD individuals to facilitate a transaction in the future, ultimately promoting ease, awareness, and accessibility. This would eliminate the recurring sentiment that cybersecurity leaders voice in having a difficult time accessing DoD officials.

To improve the cumbersome defense acquisition process and funding issues, a recently proposed and implemented solution is the OTA granting DoD authority to carry out certain developmental projects that are not a contract, grant, or cooperative agreement. Additionally, the OTA is not covered by the Federal Acquisition Regulations (FAR).[31] Since this funding option is relatively new, not many new startups or even government offices are familiar with the fund's purpose and application. Therefore, our second recommendation would be for the various DoD Small Business Offices to promote the OTA funding channel during business development meetings and technical conferences. With the 2016 National Defense Authorization Act (NDAA) Section 845, the DoD, under OTA, can award projects for research, prototype, and production purposes to traditional and nontraditional defense contractors.[32] The research category focuses on dual-use projects that would take advantage of economies of scale and bypass the Department's regulatory burdens. The prototype category focuses on weapons and weapons systems to be

[30] The AFCEA Small Business Program helps small firms with professional networking and assistance in understanding various federal policies. 'AFCEA Small Business Program' *Armed Forces Communications and Electronics Association (AFCEA).* <https://www.afcea.org/site/small-business>

[31] For details on the OTA authorities and legal guidelines, please see '(Title) 10 US Code § 2371b. Authority of the DoD to carry out certain prototype projects' *Cornell Law School - Legal Information Institute.* <https://www.law.cornell.edu/uscode/text/10/2371b> and 'Other Transaction (OT) Guide' *Defense Acquisition University.* <https://aaf.dau.edu/aaf/ot-guide/>

[32] According to Title 10 U.S. Code § 2302.9, a non-traditional defense contractor is an entity that has no current or prior minimum one-year contract or subcontract for the DoD during the solicitation period pursuant to Cost Accounting Standards – section 1502 of Title 41. For more information on Cost Accounting Standards, please see '(Title) 41 US Code § 1502. Cost accounting standards' *Cornell Law School - Legal Information Institute.* <https://www.law.cornell.edu/uscode/text/41/1502>

directly acquired or researched and developed by the Department. The production category emphasizes follow-on OT projects from an initial OT prototype project for further full-scale production purposes. Each branch of service in the DoD has the authority to implement unlimited OT projects up to $500 million with approval by the respective Service Acquisition Executives.[33]

The success of Maryland's Defense Cybersecurity Assistance Program (DCAP) can serve as a good starting model for other states to replicate in their federally funded, state-sponsored defense cybersecurity procurement programs. Maryland's model provides a well-rounded Public-Private Partnership (PPP) that bridges the defense procurement administrative process knowledge gap and the defense professional-networking gap for new cybersecurity firms entering or contemplating to enter the defense contracting market.

To further support and attract new business establishments to the state, Maryland also offers state tax incentives for pre-approved state defense cybersecurity firms on certain Maryland-produced security products. As computer and information technology hubs expand beyond the stereotypical "Silicon Valley" area of California, states such as Washington, Texas, New York, and Georgia are becoming the new technology hubs for innovation and cybersecurity. Implementing a federally-funded state program, with funds disbursed from DoD's OEA to the state's department of commerce, will help expand the DoD's search for innovation and offer an incentive to cybersecurity firms that prefer to stay in their home state due to lower tax burdens.

NSIN

We recommend that NSIN create support material like infographics that demonstrate the various pipelines for how to work with their agency, and potentially, the Defense Department as a whole (see Appendix A). For example, if an individual searches "defense opportunities for cyber startup", an NSIN workflow infographic should be one of the top search results on various search engines, which then redirects to a site containing information about contacting NSIN or other DoD agencies' business partnership offices. NSIN's marketing department can spearhead this effort by:

1) Optimizing the website so it is more popular for search engine crawls. This can be done with the inclusion of a sitemap, clear content with simplified data structure, and reasonable page size limits.
2) Adjusting the website and contents so they are more user-friendly on mobile platforms.

[33] Acquisition executives include Milestone Decision Authority, Defense Acquisition Executive, Program Element Officer, and Component (Individual Branch of Service) Acquisition Executive – Assistant Secretaries of the Army (Acquisition, Logistics, and Technology), Navy (Research, Development, and Acquisition), and Air Force (Acquisition).

3) Employing aggressive search engine ad campaigns similar to Google Smart Display advertisements' automatic targeting to reach a broader audience.[34]

The NSIN website only provides program information but not specific contact information like official office emails, business phone numbers, or a flowchart for startups to initiate the business development process. Therefore, the inclusion of the office contact information on the NSIN website and other professional network sites would help facilitate the business development process.

Conclusion

In summary, our proposals call for more defense-focused professional events such as trade shows and professional community networks, more streamlined partnership processes with alternative funding programs, more aggressive marketing and public relations campaigns, and clearer dissemination of points-of-contact information. We extrapolated from the numerous interviews with senior executives from both public and private sectors to include potential solutions for both NSIN and the DoD. The recommendations are actionable items that can be readily implemented with relatively minor changes to existing policies, standard operating procedures, and budgets. Additionally, the authorities required for most of the proposals rest within the scope of the respective office-in-charge and have already been delegated to specific office supervisors. The administrative and logistics requirements for the proposed recommendations should be relatively simple, thus making them more likely to be implemented by the respective offices.

[34] 'About Automatic targeting in Google Display ads" *Alphabet Inc.-Google.* <https://support.google.com/google-ads/answer/190596?hl=en>

Appendix A: NSIN/DoD Infographic Concept "Information for Startups Seeking Opportunities with the Department of Defense"[35]

As mentioned in our recommendations, support material identifying the different ways startups can contract with the Department of Defense could provide clarity to members of the cybersecurity startup community seeking opportunities with the Department. Graphics could also address other important topics like the Cybersecurity Maturity Model Certification. Having resources published by the DoD would contribute to the Department becoming more of a go-to resource for companies interested in engaging with USG clients. Overall, future infographics created by NSIN or the DoD should:

- Communicate the different pipelines and opportunities for cybersecurity startups to work with the Defense Department in visually-pleasing, streamlined documents.
- Include points of contact, their contact information and other links for more information.
- Design the graphic to be helpful to startups with little to no experience with federal contracting.

[35] This infographic has been designed using resources from Freepik.com Infographic vector created by freepik - www.freepik.com