U.S. Department of Defense
Office of Economic Adjustment

Project Profile: California Advanced Supply Chain and Diversification Effort (CASCADE)

Impact Statement

The OEA Industry Resilience (IR) investment in CASCADE I and II is yielding far-reaching impacts that support the defense industrial base. This Profile will not attempt to describe all activities or impacts; given that there are 15 components to each CASCADE award, the Profile instead will present key examples to illustrate the breadth and depth of the many impacts. For example, the research and analysis conducted under CASCADE I identified at least two critical findings that shaped the state's entire approach to strengthening the defense industrial base. The cybersecurity labor market and skills gap analysis documented a large gap between the demand for cybersecurity workers and the relatively few post-secondary educational programs supplying that need; and the cybersecurity provider mapping project highlighted the extensive limitations of commercial vendors to address cybersecurity compliance needs for smaller defense suppliers. Quantified impacts across 15 projects in CASCADE I alone included providing substantive assistance for nearly 4,000 defense workers and over 1,000 defense firms, touching over 80% of the 30,000 defense suppliers in the state via outreach and educational activities, and impacting over 250 communities. Finally, CASCADE developed and nurtured dozens of significant partnerships with important results across the state, responsive to each regional ecosystem, from rapidly and widely deploying an effective cybersecurity curriculum to expanding the critical talent development pipeline for space systems.

Key Project Takeaways

The Governor's Office of Planning and Research (OPR) played a leadership role in engaging key partners, defining responsibilities, and managing the many component projects. In that role, OPR demonstrated the value of state agency leadership as a coordinator and problem solver, providing quality assurance and consistent messaging. This coordination helped reinforce a statewide focus and a bias for implementation and execution built on research and analysis essential to achieving the many accomplishments of CASCADE I. OPR used a strategy of engaging trusted intermediaries to deliver services. This approach accelerated the implementation and execution because it built on existing knowledge and trusted relationships with targeted industries and companies in the defense industrial base. Their emphasis on collaboration, developing synergies, and learning from, and leveraging, other OEA grantees' and other experts' work similarly contributed to the many projects' success.

Project Description

Rationale

California plays a key role in the United States' national security posture. National security and military personnel stationed in the state contribute more than $180 billion and nearly 800,000 full-time equivalent positions to the California economy, making national security one of the state's largest economic drivers. California is home to more than 6,000 defense manufacturers and 30,000 defense suppliers, along with four Defense Logistics Agency distribution centers, the Combined Force Space Component Command at Vandenburg AFB, the Defense Innovation Unit, the Naval Information Warfare Systems Command, and other installations. These assets cross-cut economic sectors to provide key resources to the warfighter, strengthen the defense supply chain, and power the state's economy.

Uncertainty in the defense manufacturing sector since passage of the Budget Control Act of 2011, combined with the threat of foreign espionage and cybersecurity vulnerabilities, disproportionally affect California's defense firms. The projects undertaken in CASCADE I and II represent a comprehensive approach to bolster the cybersecurity resilience of the California defense supply chain, address immediate supply chain needs for California firms affected by changes in the defense industry, expand the long-term innovation capacity of California's defense industrial base, and support the growth and sustainment of California's cybersecurity workforce.

Program Activities

This Profile will focus primarily on the activities accomplished in CASCADE I (July 2017-July 2019), while noting how CASCADE II (September 2019-June 2021) builds upon experience and lessons learned from CASCADE I to generate additional and significant impacts. The onset of the Covid-19 global pandemic had varying effects on CASCADE II projects; travel and social distancing prompted many changes in approaches and enabled additional opportunities to benefit DoD and suppliers.

There are three fundamental principles that emerged consistently across all CASCADE work: 1) operating with a bias toward action including implementation and execution, as opposed to conducting research for its own sake; 2) identifying the biggest return-on-investment for small and medium defense suppliers at least cost along the most critical path; and 3) engaging a wide range of talented strategic partners that vary by project and expertise required to accomplish project objectives.

CASCADE I aimed to bolster California's defense supply chain cybersecurity resilience, innovation capacity, and diversification strategies and included 15 funded projects featuring a variety of cybersecurity resilience work, in partnership with a coalition of state agencies and community, industry, and educational institutions. OPR designed all activities to help communities respond to changes in federal defense spending, build economic resiliency, and address critical needs facing defense suppliers.

CASCADE I activity and deliverables can be grouped into three categories:

Research and Data Analysis

Cybersecurity Labor Market Analysis: The California Community Colleges Center of Excellence for Labor Market Research mapped cybersecurity workforce demand in the state, including skills in demand using the framework developed by NIST through the National Initiative for Cybersecurity Education (NICE). They identified education and training providers offering relevant skills training and produced a comprehensive report documenting findings of a growing gap between demand and supply.

Cyber Provider Mapping: CASCADE analyzed cyber providers' self-described capabilities, services, and expertise, clients they serve by size, their interest in small to medium-sized suppliers, and the cost/affordability of their offerings. They assessed the market's ability to provide critical cyber products and services related to compliance with DFARS (Defense Federal Acquisition Regulation Supplement) and examined cyber provider services in terms of the defense supplier's ability to use the solutions, including time and workforce skills. Their findings documented troubling findings about the market's inability to meet existing needs in implementing NIST 800-171 cybersecurity controls.

Education and Outreach

Regional Resilience Workshops and Resource Fairs: CASCADE hosted seminar series tailored to multiple regional ecosystems to foster supply chain resiliency and focus on industry verticals with ties to defense spending. The grass-roots approach worked to understand unique regional needs, service providers, and tailored strategies and agendas accordingly. In partnership with other CASCADE projects, these workshops provided business planning and market exploration to enhance the cybersecurity resilience of defense suppliers, build awareness about cybersecurity and workforce development, and support modernization and diversification efforts.

Business Assistance and Workforce Development

Cybersecurity Bootcamps: CASCADE designed supply chain cybersecurity training modules in collaboration with DAU, DCMA, and the NIST MEP network. CASCADE hosted bootcamps to increase awareness about cybersecurity threats for SMMs (threats from adversaries and threats for noncompliance with federal regulations like DFARS). The bootcamps helped to increase awareness, identify opportunities for SMMs to access resources that can increase resilience to cyber threats, and support the cybersecurity, modernization, and diversification efforts of California-based DoD stakeholders. CASCADE I and II held two-day training sessions in 2019 and 2020 for organizations that are OEA recipients and/or NIST MEP Centers from over 20 states. This collaborative cross-training provided many with their first direct experience in cybersecurity with DoD Acquisition commands. DAU and CASCADE provided training, standardized methodology and content for these attendees to take back for defense suppliers in their states.

Cybersecurity Assessments: It became evident that most small and medium-size DoD suppliers would not, or were unable to, address cybersecurity issues without support. Building off the cyber-resilience workshops, CASCADE conducted deep dives with various defense suppliers by assessing and documenting cybersecurity capability and readiness to both defend against cyber threats and prepare the suppliers to comply with DFARS-required cybersecurity controls. To modernize and enhance the cybersecurity resilience of the defense supply chain, CASCADE developed and refined a Cybersecurity Assessment Framework specifically tailored for the needs of smaller defense suppliers.

CASCADE II builds on these activities and bolsters California's defense supply chain resilience through cybersecurity preparedness assistance programs and support for growing and sustaining its cybersecurity workforce. It again incorporates a wide array of partner organizations across 15 individual projects including work on education curricula, training, internship, and apprenticeship programs, and broadening capabilities and reach through train-the-trainer networks. Specific projects include:

- Guidance on Cyber Provider Services
- Cybersecurity Resilience Workshops
- NIST MEP Cybersecurity Cross-Collaboration Initiative
- SBDC & PTAC Network Cyber Resiliency
- Cybersecurity Baseline Compliance Evaluations
- Cybersecurity Compliance Implementation & Execution
- Cybersecurity for Space Systems
- Industry Cybersecurity Workforce Strategy
- Cyber Career Commercial Pathways
- Defense Workforce Cybersecurity Skills Upgrading
- Community College Collaborative Cybersecurity Workforce Initiative
- Cybersecurity Internships/Externships with DoD SBIR/STTR Firms
- Cybersecurity Apprenticeships
- Cybersecurity Job Placements

One unique effort involves Project 8, Cybersecurity for Space Systems. California Polytechnic State University, San Luis Obispo (Cal Poly SLO) is leading an effort to better understand a top priority for national security, enhancing the cybersecurity of space assets. Space is now considered a warfighting domain because much of U.S. critical infrastructure relies on connectivity in or through space. The California Cybersecurity Institute at Cal Poly SLO project addresses identified DoD and commercial space needs in many ways. Two important components include conducting a Space Operations Challenge series and two Space Summits leveraging Cal Poly's Digital Transformation Hub (DxHub) in partnership with Amazon Web Services (AWS) to leverage innovation methodologies with subject matter and technology expertise. The challenges are varied, including small satellite design, multi satellite launch capabilities, secure space communication, cloud-based space data processing and analysis, secure satellite command and control, and education and workforce development opportunities for space and cybersecurity. This project alone engages more than 20 partners, including DoD's Office of the Secretary of Defense (OSD), United States Strategic Command (USSTRATCOM), and the Vandenberg Air Force Base 30th Space Wing Air Force Space Command.

Resiliency Impacts

Increasing Awareness of the Defense Industrial Base

The Governor's Office of Planning and Research plays a critical leadership role in building, organizing, and sustaining a network of service delivery partners and stakeholders across the state. The breadth and depth of this coalition, reaching into communities across the state, increased awareness about the extent of the defense industrial base, the needs of defense manufacturers, and opportunities to address those needs. OPR was focused on identifying and qualifying providers and partners that share their bias toward action and execution to generate impact. Over the course of CASCADE, OPR and sub-awardees have touched about 80% of defense suppliers in the state's DIB, evidence of the extent to which the collective effort engaged those partners across all projects and increased awareness.

OEA support played a critical role in developing California's understanding of its defense industrial base. Previous IR grants to the San Diego grantee funded the development of the Connectory, a database of defense suppliers. Leveraging the Connectory, CASCADE partnered with California State University at San Bernardino (CSUSB) to conduct outreach through the Connectory, websites, and the networks of over 50 economic development and industry agencies. CSUSB surveyed defense suppliers to identify those at risk to changes in defense spending. The California team used this data to expand its listing of defense suppliers; the Connectory now serves as a database of defense firms for statewide partners.

Supply chain mapping expanded California's awareness of its defense industrial base, facilitating CASCADE's outreach to suppliers with critical business support services. These activities support DoD resiliency by improving California's ability to target defense suppliers and regions heavily impacted by changing DoD priorities with support services to find new markets, improve their capacity, or support the workforce. CSUSB also mapped the Lockheed Martin Skunk Works supply chain, a highly classified DoD aerospace program, and produced a defense spending impact model to estimate the regional impact of changes in defense spending.

Increased awareness of the DIB by key DoD assets illustrates another benefit to DoD. Despite their classified mission, Skunk Works demonstrated their awareness by reaching out to the supply chain at a Supplier Resiliency Workshop to offer opportunities and leverage innovation residing in smaller California suppliers.

Enhancing Force Multipliers to Support the Defense Industrial Base

CASCADE's partners generally include economic development agencies, CMTC (the state's MEP Center), SBA district and SBDC offices, PTAC offices, Chambers of Commerce, state agencies and higher education institutions, municipalities, and financial institutions. Over 100 organizations partnered with CASCADE in supporting the defense industrial base. One notable example of how partners build the capacity of community intermediaries and enhance force multipliers is the CASCADE II Project 5 with the San Diego East County Economic Development Council (ECEDC). ECEDC is building the capabilities of SBDCs, PTACs, and community colleges to assist in educating and training workers, advisors and faculty about cybersecurity requirements and assisting companies in assessing and addressing risks.

With technical support from CMTC, ECEDC is developing a decision tree to help regional stakeholders and service providers guide small defense suppliers to resources that facilitate suppliers' implementation of cybersecurity controls. They plan to introduce the importance of addressing cybersecurity risks as a competitive advantage during business consultations and address the lack of business support professionals with an understanding of cybersecurity. ECEDC plans to create a cybersecurity how-to guidebook and offer train-the-trainer sessions at statewide SBDC or PTAC meetings to increase the number of business support professionals that understand businesses' cybersecurity needs. This project aims to offer practical solutions and guidance to PTACs to advise small business clients on cost-effective approaches to cybersecurity compliance. This project increases the capacity of regional assets to provide cybersecurity preparedness support to small defense suppliers, both sustaining the defense industrial base and facilitating entry by small businesses.

Cost Savings to DoD through Business Diversification or New Products/Customers

OEA IR investments in CASCADE generated cost savings to DoD generally in two forms. The first involved the many defense suppliers that received the highest value, highest impact services at reasonable cost because of information provided by CASCADE and its partners. The cybersecurity provider mapping research (CASCADE I, Project 3) found that many suppliers were not taking cybersecurity seriously, or if so, they were sometimes paying large consulting fees for vendor services that were not equipped to deliver support for NIST 800-171 compliance activities. The CASCADE partners worked extensively to understand the perspective and needs of small and mid-sized defense suppliers, to develop and deploy information in awareness sessions and through hand-on technical assistance, and to help those suppliers realize the biggest return-on-investment at the least cost. This approach likely resulted in reduced costs for cyber compliance passed along to prime contractors and ultimately, to DoD.

CASCADE II's efforts to develop cybersecurity provider guidance directly built on the CASCADE I Cybersecurity Provider Mapping Effort. The Guidance on Cyber Provider Services (CASCADE II, Project 2), is using research gathered on cyber providers' capabilities and specialties to create a guidance structure for defense suppliers seeking a cybersecurity provider. The methodology will consider a company's needs and capacities, with respect to implementing NIST 800-171 controls, to help defense suppliers identify the provider that meets their specific needs. This guidance tool will provide cost savings to firms', by helping them match with the appropriate provider for their needs and capacity, and ensure the firm works with a provider that facilitates their compliance with DFARS 252.204-7012.

The second way that IR grants generated likely DoD cost savings involved those defense suppliers that implemented steps to comply with DFARS and reduce their cyber risks by participating in cybersecurity preparedness bootcamps, technical assistance, and training. Those companies are better prepared to prevent or withstand cyber-attacks and to recover more cost effectively when attacks do occur. Moreover, the defense suppliers' awareness and preparedness can reduce costs related to loss of controlled unclassified information (CUI), trade secrets, and business intelligence to competitors or adversaries. Finally, companies that are cyber compliant are better positioned to maintain and/or expand business in the defense supply chain over competitors that are not meeting established standards.

Lethality Impacts

Innovation Through the Development of New Intellectual Property or New Technologies

CASCADE's partnership with Cal Poly SLO and AWS through the Digital Transformation Hub (DxHub) Cloud Innovation Center (CIC) is among the most innovative IR-funded projects The Space Operations

Challenge series is addressing numerous challenges with implications for DoD lethality. These include small satellite design, multi satellite launch capabilities, secure space communication, cloud-based space data processing and analysis, and secure satellite command and control. Vandenberg Air Force Base and Cal Poly signed an Educational Partnership Agreement to execute the Space Operations Challenge series and train students in crucial technologies in-demand by the DoD.

The small satellite design challenge, of great interest to Vandenberg Air Force Base (VAFB), aims to accelerate the time to launch for silo missions by using commercial vendors' satellites equipped with DxHub-designed secure communications transmitters that meet DoD standards. DoD satellites can take as long as 10 years to develop and up to 5 years to receive launch approval, a schedule that is untenable for small satellites that might only last 2 years in orbit. Commercial vendors time-to-launch is a fraction of the DoD's; leveraging this commercial capacity is a vital opportunity for the DoD to access the benefits of small satellite constellations while collecting data from a larger number of vendors.

The DoD can then leverage non-traditional data collected with defense-specific telemetry data. Vendors similarly benefit as DoD contractors. Managing securely transmitted data on a secure cloud removes problems associated with compiling big data from numerous satellites and sensors through leveraging increased computing power and ensures data is analyzed on a secure cloud platform, limiting the need to develop new cybersecurity protocols. Eventually this could lead to providing real-time data to assess impact areas, from fighting forest fires to conducting battlefield assessments. Moreover, it could provide replicable solutions that VAFB can share with other bases to decrease costs and time-to-launch. As this approach grows, the risks of ensuring secure communications and control will also increase. This challenge leverages Cal Poly encryption expertise to secure commercial platforms[1].

Readiness Impacts

Training and People Support

The CASCADE I California Cybersecurity Labor Market Analysis captured important data and enhanced the state's understanding of the workforce shortage and skills gap in filling cybersecurity positions. The study found an alarming gap in the supply of qualified cybersecurity workers prepared to fill more than 37,000 cybersecurity-related annual job openings that exist in California. The report highlights that "finding qualified workers to fill cybersecurity positions is a widespread challenge facing many employers particularly, defense contractors, across all industries." The issue is compounded by the fact that California's educational institutions are not currently supplying enough qualified candidates to fill the thousands of cybersecurity job openings that exist; California only has 61 cybersecurity-focused education programs, producing only around 3,200 cybersecurity candidates annually. More recent data suggest that the number of cybersecurity openings is more likely closer to 72,000 positions. CASCADE II

[1] Cal Poly will submit a prototype for the next SBIR/STTR cycle for development as dual use technology. See demo video here: https://youtu.be/45Ro_bX4Q50

leveraged this increased understanding of the state's cybersecurity workforce to design a series of cybersecurity workforce programs that address every level of the cybersecurity workforce pipeline.

As noted above in describing how CASCADE is expanding force multipliers, San Diego East County Economic Development Council (ECEDC) is engaged in training cybersecurity trainers for community colleges, PTACs, and SBDCs under CASCADE II, Project 5. No doubt this has implications for raising worker and company leader skill levels broadly around cybersecurity.

The Space Operations Challenge Series (Project 8) described above includes education and workforce development opportunities for space and cybersecurity. An Educational Partnership Agreement (EPA) made collaboration among higher education institutions possible. This leveraged a strong digital workforce initiative called "California Strong Workforce" across all community colleges in the state. In addition, Cal Poly SLO plans to leverage the findings from the work to design training, degree and certificate programs that address critical workforce skills gaps in these fields, with great potential to support the readiness of defense suppliers in supporting new DoD missions. Additionally, engaging Cal Poly computer science students in support of these challenges provides students with practical experience in supporting DoD-related technology challenges and exposure to employment opportunities in a field of critical demand for the long-term DoD strategic objectives.

The Council also leads developing an industry-driven cybersecurity workforce strategy (CASCADE II, Project 9) and building experiential and work-based learning opportunities based on best practices and models for cybersecurity apprenticeships (CASCADE II, Project 14). The strategy identified that experiential learning is a major gap to increasing the pipeline of qualified cybersecurity workers.

ECEDC partnered with the California Cyberhub at synED to develop job placement, competency-based apprenticeship programs, and employee development programs that provide workers with the skills needed to fill California's 72,000 open cybersecurity jobs. Many cybersecurity providers fail to fill critical roles because candidates lack the experience or skills desired by firms. SynED partnered with Apex Systems, an information technology staffing agency, to leverage an on-the-job training model that upskills IT workers to develop in-demand cybersecurity skills. They adapted an on-the-job training (OJT) model using assessment tools and training models developed by the National Cyberwatch Center. SynED's efforts meet cybersecurity providers halfway, by providing candidates with the required skills to fill roles, without the desired years of experience hard to find in the labor market. Apex Systems is also looking to use an Apprenti-developed apprenticeship model specifically for defense IT workers. Additionally, synED has partnered with managed service providers and managed security service providers to build apprenticeship or training programs specifically for entry-level job candidates. CASCADE I research found many cybersecurity providers are unaware of DFARS cybersecurity controls, making it crucial to help firms hire talent both aware and capable of implementing NIST 800-171 controls. Additionally, OJT increases cybersecurity employee retention in a field that typically experiences high turnover. Cybersecurity apprentices or trainees that gain that valued one-year of experience can remain with the cyber provider or be placed with an employer such as a DoD supplier.

The partnership with Apex Systems closes the loop by providing the staffing services to place now experienced cybersecurity workers.

Project 10 Cyber Career Commercial Pathways – Under the CASCADE II project, Cyber Center of Excellence (CCOE) and the State of California are partnering with Journeys Map on an interactive pilot to map cyber education, trainings, certifications and career pathways. Cyber Career Map users can chart personal paths to a cyber career with the exploration dashboard and zoom in for jobs, education, resources and much more. The Cyber Career Map includes NICE/NIST cyber crosswalks, national certifications, California university and college curriculums as well as military to commercial pathways. To complement and promote the Cyber Career Map, CCOE is hosting Link2Cyber programs at universities and colleges to connect high school and college students, transitioning service members and veterans with career opportunities through industry-led panels. To date, the effort has engaged 280 students and 20 employers, generating 223 new Cyber Career Map users.

To promote adoption and awareness of this new resource as well as critical cybersecurity preparedness issues, CCOE also developed the Cyber Insiders Podcast Series on iHeartRadio to tell the story of California's cyber economy, current threat landscape, protection and risk management strategies, cyber innovations, and workforce needs. The 10-part series features leaders from industry, academia and government agencies. The first 6 episodes generated 430 downloads.

Project 11 Cyber Skills Upgrading -- One of the most well-established state-funded training programs in the nation, California's Employment Training Panel (ETP), assists employers in strengthening their competitive edge by providing funding to offset costs for job skills training. ETP is a co-investor in CASCADE, committing over $230,000 in cash and in-kind services to address three key elements: (a) Cybersecurity training consistent with federal partners' requirements, (b) Resiliency within the defense supply chain including computer skills training, continuous improvement, and manufacturing job skills training. (c) Entrepreneurial skills training including cyber-awareness for the owners of supply chain employers employing 10 or fewer full-time employees.

Project 12 The Collaborative Cyber Workforce Initiative worked with DoD's Defense Acquisition University and prior OEA grantee Propel San Diego to develop a training curriculum of cybersecurity courses for the defense workforce. The employer-validated curriculum was piloted at El Camino Community College then made available to community colleges statewide. This project also delivered train-the-trainer sessions engaging the California Community College Contract Education Collaborative (CCCCEC) colleges, regionally dispersed community colleges in a variety of counties near military installations. The CCCCEC includes over 30 colleges that offer contract education to industry throughout California and provide reach to all 115 community colleges. In effect, all 115 colleges will have access to all the curriculum developed to adopt it into training and educational programs as they see fit. Thus far, 20 of the colleges with a high concentration of DoD suppliers in their region have committed to participating in the project and offer cybersecurity training. Marketing efforts anticipate reaching over 200 DoD suppliers, with many sending employees to these trainings paid for by ETP state funds.

Project 13 Cyber internships/externships with DoD SBIR/STTR – This project is placing community college student interns coached by faculty externs at California DoD SBIR companies to assist them with cybersecurity readiness and compliance. Students benefit from the opportunity to apply knowledge from their educational programs and gain real world experience. Faculty benefit from bringing industry experience back to the classroom. An anticipated 40-60 student interns and 20 faculty mentors/coaches from nine colleges across the state will participate in the student internships at 20 DoD SBIR/STTR firms. As centers of defense innovation, it is especially important that SBIR/STTR awardees have access to this added cybersecurity expertise and assistance.

Improved Capability and/or Production Adjustments

CASCADE's cybersecurity activities greatly improved defense suppliers' capabilities to withstand cyber-attacks. These impacts are discussed in detail below.

Cybersecurity Preparedness

OEA's investment in CASCADE produced an ambitious and comprehensive approach to addressing cybersecurity risks in the defense supply chain. CASCADE provides a model for engaging and deploying resources at the state, regional, and local levels to help address these issues and advance critical DoD objectives, including various National Defense Authorization Acts (NDAA), the National Cyber Strategy, the National Defense Strategy, and cybersecurity clauses in the DFARS.

Project work conducted under CASCADE I demonstrated critical issues that DoD will need to address to enhance cybersecurity compliance and mitigate risk, including: (1) Cyber threats to defense suppliers pose a significant risk to national security, (2) Suppliers lack adequate insight into existing cyber postures, DoD/CIO objectives, and DoD cybersecurity regulations, and (3) Defense contractor capabilities to address cyber threats must address the shortage of qualified cyber workers.

CASCADE made significant progress on education about DFARS Clause 252.204-7012 and implementation of best practices/standards in NIST 800-171 Rev 1 cybersecurity requirements, guidance on cyber provider services, and defense cybersecurity workforce development. As noted above, quantified impacts across 15 projects in CASCADE I alone included providing substantive assistance for nearly 4000 defense workers and over 1000 defense firms, touching over 80 percent of the 30,000 defense suppliers in the state via outreach and educational activities, and impacting over 250 communities. Over 750 defense firms attended CASCADE I cybersecurity preparedness bootcamps and workshops, and 28 companies began implementation of their cybersecurity preparedness programs thanks to services provided by CASCADE and its partner, CMTC.

Throughout its cybersecurity preparedness support for defense suppliers, CASCADE uses strategies that identified the biggest return-on-investment for participants, based on experience in CASCADE I, input from suppliers and the expertise of CMTC's cybersecurity consultants. They tailor the message in large group sessions to supplier company priorities, including profitability, growth, trust, and workforce/

technology issues to help firms realize the benefit of adopting cybersecurity controls for their business' operations and profitability. Their approach to each requirement is based on an identified use case and a critical path for addressing it at least cost. This involves helping defense suppliers identify what type of information qualifies as CUI and develop a multi-tier system architecture that only secures covered-defense information. This limits defense suppliers' cost and level-of-effort in implementing increased cybersecurity controls, while facilitating their compliance with DFARS. CASCADE provides opportunities to follow-up with individual companies to reinforce action steps and support progress and help companies develop their own cybersecurity capacity.

Impresa Aerospace, a Gardena, CA 200-person sheet metal supplier of wing parts and components for Boeing and other commercial and defense OEMs, initially approached an accounting firm for a cyber compliance audit after a ransomware event. The accounting firm's 3rd party cyber-provider proved costly and did not result in the company's implementation of DFARS compliant cybersecurity controls, leaving Impresa vulnerable to the loss of its DoD contracts. After attending a CASCADE-sponsored bootcamp, they worked in partnership with CMTC at one-third the cost for remediation and compliance to raise awareness among its employees, provide training, and establish critical processes for ongoing DFARS cybersecurity compliance. This support resulted in Impresa hosting its cybersecurity capacity in-house, decreasing its costs relative to an external provider. Impresa envisions a "significant competitive advantage" in competing for DoD contracts with the inclusion of CMMC accreditation in DoD contracts.

More broadly, three CASCADE I projects illustrate approaches used to understand the challenges and meaningfully engage defense suppliers around cybersecurity awareness and risk mitigation.

In the cyber provider mapping project (Project 3), CMTC studied the cyber provider marketplace and assessed the ability of existing vendors to provide critical cyber products and services related to DFARS. Their report yielded unpromising findings. Researchers found that commercial cybersecurity vendors face significant barriers to addressing compliance needs for smaller manufacturers and other suppliers in the defense industrial base, including lack of tools and/or curriculum customized for small- and mid-sized suppliers, and lack of interest in or financial incentives for serving that market.

CASCADE II's Guidance on Cyber Providers (Project 2) directly builds from this effort and hopes to provide defense suppliers with the tools to select cybersecurity providers that meet their needs.

CASCADE I Projects 8 and 9: CMTC held five cybersecurity workshops, or "bootcamps," over 18 months in locations near concentrations of defense suppliers, and close to DoD Acquisition offices and Command centers. CMTC additionally provided direct NIST 800-171 cybersecurity preparedness services to defense suppliers (Project 9) that helped suppliers develop and implement NIST 800-171 cybersecurity preparedness plans. The cybersecurity change-management model deployed by CMTC follows the DAU training model. CASCADE was able to identify companies in-need of cybersecurity services through the Connectory and its previous defense supplier survey, as part of the supply chain mapping project. Interactions with suppliers in bootcamps and consultations had three major impacts: 1) they shattered DoD and CMTC assumptions from 2017-2018 that small and medium-size DoD suppliers had a reasonable understanding of CUI/CDI, how to protect that information, and how to pursue DFARS cyber compliance; 2) they shattered the assumption that DoD contractors did not use digital cloud systems that may invoke additional DFARS cybersecurity regulations and requirements; and 3) they informed CMTC and CASCADE strategies for developing effective outreach, education, assessment, and technical assistance. Over 750 defense suppliers received cybersecurity preparedness guidance through CASCADE workshops and bootcamps, and 28 suppliers began to implement their NIST 800-171 cybersecurity preparedness plans to become DFARS compliant.

CASCADE II continues this work in several ways. Continued cybersecurity preparedness workshops (Project 3), provision of cybersecurity baseline evaluations (Project 6), and compliance implementation and execution (Project 7) all help firms implement NIST 800-171 controls, become DFARS compliant, and develop the capacity to support their cybersecurity infrastructure themselves.

CMTC's one-on-one cybersecurity services consist of three phases. The first phase, incorporation, helps firms understand the need for cybersecurity controls, including providing a baseline evaluation of the firms' cybersecurity posture and the creation of a schedule to implement controls. The second phase, implementation, involves the provision of technical assistance to defense suppliers to institute NIST 800-171 controls according to the most critical path at the least cost. This typically involves identifying CUI and segmenting it from unsecure portions of a firms' network. The third phase, execution, is intended to help companies develop their own cybersecurity capacity, including the development of documentation, processes, performance measurements, and reporting tools for its appropriate cybersecurity posture, allowing firms to continue to maintain DFARS compliance. CMTC training reduces the hours associated with NIST 800-171 implementation from 600 to 200 hours.

Most recently, CASCADE has helped defense suppliers and the DoD understand the increased vulnerabilities to the defense industrial base due to Covid-19. Increased teleworking and more relaxed employee behaviors at home have magnified the attack surface and frequency from China, Russia, and Iran. The threats from delayed deliveries, disrupted supply chains, and the lack of diversified sourcing are magnified. Critical nodes in the DIB that smaller businesses provide are at risk from the financial impacts of the virus. The current environment increases the potential loss of suppliers across the DIB and risks of foreign acquisition of defense suppliers and critical technologies through predatory and adversarial capital and cyber-attack. Cyber-attacks in this environment could potentially increase the DIB dependence on foreign production, a threat to DoD supply chains that requires mitigation.

In response, CASCADE partners are working to help suppliers better manage CUI on personal networks. Cyber student interns that had been placed with defense suppliers have moved to working with them remotely. CASCADE partners are working with expanded partnerships with NDIA to understand industry impacts, and with the Defense Innovation Unit and AFWERX and NavalX to accelerate the acquisition process moving goods from California-based suppliers to DoD. This highlights one of the lasting benefits of CASCADE -- the increased cooperation and collaboration among the network of partners working towards broader cybersecurity resilience.

Other Community Benefits

Alignment with State Programs

California's Office of Planning and Research led both CASCADE I and II grants. OPR's position within the Governor's office provides authority when engaging with partners and attracts support from organizations across the state. For example, OPR engaged senior state and Vandenberg AFB officials to facilitate an environmental review through OPR's land management office to help Vandenberg develop launch infrastructure. Moreover, partnerships with defense entities and installations further increase CASCADE's sense of legitimacy when engaging with defense suppliers, a crucial factor in attracting firms to their support services.

Activities are executed via many direct partnerships with government, industry, community, and academic institutions across the state and beyond. The leads for each project create relevant state and national partnerships to execute assigned work. Those strategic partners vary by project but generally include economic development agencies, SBA district and SBDC offices, PTAC offices, Chambers of Commerce, state agencies and higher education agencies, municipalities, and financial institutions. OPR's leadership and project management approach ensure that organizations involved in these partnerships are aligned with state programs and DoD strategies, particularly regarding emerging guidance on cybersecurity compliance in general and CMMC in particular.

As just one example, the team selected to work on the research regarding cyber provider mapping and the cyber DFARS bootcamps and assessments (CASCADE I Projects 3, 8 & 9) included DAU, NDIA, NIST MEP National Network, ISACA[2], National Contract Managers Association, MITRE, Navy SPAWAR[3], various SBA small business offices, SBIR/STTR programs, DIU, California Military Department, the California Cyber Integration Center, U.S. Department of Commerce/Commercial Service, and the DHS Critical Manufacturing Sector. The CASCADE II Cybersecurity for Space Systems effort (Project 8) has already engaged with over 25 organizations including educational institutions, aerospace firms, and military installations. Other CASCADE projects engaged similar sets of expert organizations and individuals.

CASCADE partners additionally leveraged CASCADE's authority as a component of the Governor's Office and its partnership with military installations to engage in cybersecurity training activities beyond the grant. Cal Poly partnered with the California National Guard's Camp SLO, which hosts the California Cybersecurity Institute (CCI), to provide a high school cybersecurity competition that also engages students from Cal Poly. A portion of this competition is funded by the NSF Gen Cyber and has attracted interest from D.C. organizations such as R Street. The CCI's week-long High School Cyber Challenge engages students in a forensic analysis of a cyber-attack and relies on the NICE framework and input from partners such as the National Security Space Association and JPL to develop the programming.

[2] ISACA is a professional association with 145,000 members around the world who have responsibility for information technology assurance, risk, governance, and information security.

[3] Space and Naval Warfare Systems Command (SPAWAR) has changed its name to Naval Information Warfare Systems Command (NAVWARSYSCOM) reaffirming the command's commitment to outpacing adversaries in the information warfare domain to enable a competitive edge in all other warfare domains.

Previous programming simulated a cyber-attack on pacemakers, and this year's programming will simulate a cyber-attack on a satellite.[4] Cal Poly students develop the competition and are exposed to new employment opportunities with the DoD, including in fields such as videography/photography, graphic design, and engineering. These students play a key role in translating cybersecurity to a non-technical audience and increasing the profile of cybersecurity issues. Cal Poly's relationship with the CCI also resulted in internships for students to train in and utilize Splunk, a cybersecurity platform that is in-demand by many organizations, including the DoD.

Cal Poly's relationship with Camp SLO also resulted in key benefits to the California National Guard, whose Cyber Protection Team 171 (CPT) is responsible for responding to cyber-attacks on state-government infrastructure. With funding from the Hewlett Foundation, Cal Poly and the CCI increased the capacity of the Cyber Protection Team to respond to cyber-attack, including against ransomware attacks on government systems and critical infrastructure. Grant funding paid for some of the Team's training, and the partners expect more funding over the next few years. The protection services provided by the CPT are critical in supporting the defense industrial base, which ultimately relies on government services and utilities-infrastructure to operate and support the DoD.

Lessons Learned

Greatest Challenge

OPR cited several challenges encountered with the CASCADE projects. The single biggest challenge has been the rapidly changing environment related to compliance with DoD cybersecurity rules and directives. Understanding DoD policy and assessing how to translate policy changes into workable knowledge for suppliers have been difficult. Similarly, it is challenging to develop and deploy consistent messaging for all partners and stakeholders and defense suppliers about how to implement DoD directives. Advising smaller defense suppliers on how to finance needed changes is also a barrier to progress. Finally, it is difficult determining optimal approaches for how to execute effectively and scale programming while retaining high quality standards across multiple locations.

Most Important lessons learned

Across the projects of CASCADE I and II, there are many lessons learned for DoD and others providing cybersecurity services to strengthen resiliency and reduce cyber risks among the DIB. These include:

1. Understand your region's cyber landscape. It is important to take the time to assess the unique needs of defense suppliers and the capabilities of service providers, and develop, implement and execute strategies that address that landscape.
2. Balance DoD priority inputs. The cybersecurity environment is changing especially rapidly. With guidance and information coming in from DoD, DAU, acquisition commands, industry, MEPs,

[4] This year, the challenge will also be available to 1,000 participants at Aerospace Village at DEFCON.

PTACs, and others, it is critical to figure out how to balance all the info coming in and determine when and how to incorporate it into ongoing efforts.

3. Focus on training, technical assistance, and workforce development if you want to move the needle. CASCADE's emphasis on implementation and execution demanded that the projects engage in activities that would generate impact with defense suppliers, defense communities, and defense workers. These activities generated the most progress on important objectives.
4. Develop a strategy for determining which defense suppliers should receive intensive services first. OPR and partners determined that using first come, first served is neither strategic nor effective. Offering different tiers of services based on DoD priorities is a preferred approach that ensures that companies that demonstrate evidence of working on critical DoD programs make progress against goals.
5. Beware of cyber providers and cyber consultants that want to help. CASCADE research studied the ecosystem of consultants extensively and found numerous reasons why they were unable to meet the needs of small and mid-sized suppliers. CASCADE recommends working with MEP Centers and other trusted intermediaries first.
6. Appeal to profitability, growth, trust, or workforce and technology concerns to get the attention of small and mid-sized suppliers to address cybersecurity risks. Bring small firms into the conversation by combining cyber information tied to future business opportunities. Trying to sell cybersecurity compliance for its own sake is not effective and didn't generate desired results.
7. The network of relationships built under CASCADE I and II proved invaluable when Covid-19 hit. While adjusting project plans to reflect new constraints, the CASCADE team identified new ways to benefit DoD and the DIB as their supply chain threats, external threats, and internal threats changed. These included educating suppliers about the additional vulnerabilities of telework and videoconferencing, as noted above, and assisting U.S.-based manufacturers to shift production capability to address the military and federal employee need for personal protective equipment. CASCADE in conjunction with CMTC formed new relationships with the U.S. Air Force AFWERX Program and the Federal Executive Board of Greater Los Angeles, which is led by local Department of Homeland Security executives, to source domestic suppliers of PPE where critical health care industry needs have depleted existing stockpiles. As PPE needs are satisfied, this initiative will shift to other areas of U.S. domestic need for DoD and Federal customers that may replace projects from foreign sources.