U.S. Department of Defense
Office of Economic Adjustment

Project Profile: Colorado Springs

Impact Statement

The Colorado Springs grantee is building the ecosystem of support for the region's extensive array of military installations and defense suppliers, focusing on growing the pipeline of skilled technical workers to address cybersecurity needs to the benefit of DOD and the warfighter.

Key Project Takeaways

As an Industry Resilience (IR) grantee, the Colorado Springs IR team launched the Pikes Peak Regional Defense Assistance and Defense Diversification Program to unite regional efforts around the development of a Colorado Springs cybersecurity ecosystem that provides opportunities for businesses, workers, students, and transitioning military members. The cultivation of a robust cybersecurity ecosystem in Colorado Springs benefits national security by growing the pool of talented cybersecurity professionals available for both DoD and defense contractors' operations, and augmenting cybersecurity provider's capacity to secure both DoD and defense contractor's sensitive information. These activities directly benefit the DoD's ability to increase its resiliency and readiness. The alignment and growth of the cybersecurity ecosystem in Colorado Springs spurred by the IR Grant can augment the DoD's capacity to operate in the "Fifth Domain," while securing DoD assets from becoming compromised by cyber-attacks.

Project Description

Rationale

Colorado Springs is a heavily defense-dependent region, with over 55,800 direct employees associated with the military installations at Fort Carson Army Post, Schriever Air Force Base, Peterson Air Force Base, Cheyenne Mountain Air Force Station, and the U.S. Air Force Academy. A sizable defense contractor base also exists, primarily in the areas of command & control, space and satellite operations, information technology, and cybersecurity. A recent study identified the aerospace and defense industry's direct and indirect impact on the Colorado Springs MSA as 44% of the overall economy. Cybersecurity alone accounts for 1.4% of employment (6,285) and 2.7% of Colorado Springs' GDP, with a vast majority of the 125+ firms reliant on DoD contracts. Regional average wages in cybersecurity are $104,000, more than double the local average wage. Despite lucrative opportunities in cybersecurity, it is estimated that 7,000 cyber security jobs are needed in the workforce to sustain the ecosystem. With the Colorado Springs cybersecurity industry and the overall economy so reliant on DoD expenditures, any reductions to the DoD budget pose a significant threat to the region's industries. Without a robust supply of cybersecurity workers, the existing defense contracting work and DoD operations in the region may lack the capacity to support national defense. Regional military installations already face a shortage of cybersecurity professionals to secure legacy systems. Growing opportunities for cybersecurity firms outside of defense bolsters their ability to survive any fluctuations to defense spending and provides opportunities for cybersecurity workers waiting on the clearance necessary to support DoD contracts. In response, Pikes Peak Community College (PPCC), the Colorado Springs Chamber, and the Economic Development Council (EDC) sought OEA funding to develop a comprehensive strategy to promote opportunities for businesses, students and workers in the cybersecurity industry, seeking to establish Colorado Springs as a nationally recognized hub for cybersecurity.

Program Activities

To diversify its economy and support workforce needs in cybersecurity, the Pikes Peak Regional Defense Assistance Program pursued several activities. One set of activities led to the development of a coordinated cybersecurity strategic plan for the region. The planning process was led by the Colorado Springs Chamber & EDC and important tasks related to the effort included completing:

- Matrix of Stakeholders' Cybersecurity Strategies
- Asset Map of Colorado Springs Cybersecurity Industry and Service Providers
- Asset Map of Key Regional Leaders/Stakeholders Necessary to Successfully Implement the Cybersecurity Strategy and their expertise
- Analysis of Separating Military Skills and Certifications, cross-walked to industry certifications
- Review, Adoption, and Public Roll-Out of Cybersecurity Strategic Plan by Stakeholders
- Development of a Cybersecurity Coordinating Committee representative of the region's cybersecurity stakeholders

Using the IR grant, the Colorado Springs Chamber & EDC contracted with the outside consulting group Simon Everett to develop the strategic plan. The final cybersecurity plan includes specific recommendations for the region to successfully align its cybersecurity ecosystem, provide diversification assistance to defense contractors, and cultivate a well-trained cybersecurity labor force. These activities benefit the warfighter by providing a larger pool of "cyber-warriors" able to support DoD operations and secure DoD contractors. A larger, more talented pool of cybersecurity professionals addresses the workforce shortage inhibiting DoD operations, and provides increased capabilities for the DoD.

A second set of activities sought to secure the designation for Pikes Peak Community College as a National Security Agency (NSA) Center of Academic Excellence 2-Year (CAE2Y) and to expand the institution's cybersecurity industry-related training. Important tasks related to this outcome included completing:

- Cybersecurity Skills Gap and Labor Market Survey
- NSA-Compliant Academic Degree Program Outline
- AAS Degree Programs in Cybersecurity and Network Security Approved by PPCC and Colorado Community College System
- New Academic and Non-Credit Courses Developed
- Cyber Range Plan
- NSA CAE2Y Designation
- Launch New Degree and Certification Programs in Applied Cybersecurity
- Establish a formal DoL apprenticeship program in cybersecurity

This CAE2Y designation was established by the National Security Agency (NSA) and the Department of Homeland Security (DHS), with the support of the National Science Foundation (NSF) and CyberWatch.

Community colleges that have established a robust information assurance (IA) program and have successfully mapped their security courses to two of the Committee on National Security Systems training standards are eligible to apply for this status. Five institutions in the region have NSA CAE designation, with the University of Colorado-Colorado Springs (UCCS) working toward a second designation in research. Much of the work done by PPCC benefits former service members, many of whom will continue to support DoD operations as an employee or contractor after receiving an education, enhancing workforce skills, or changing careers. PPCC has established an AAS in Cybersecurity and has had a 400% increase in enrollment during the first two years of the program.

Throughout this work, officials from PPCC and Colorado Springs Chamber and EDC worked with educators and officials to supplement and align cybersecurity efforts and reduce duplication. Outreach to local high schools resulted in the adoption of cybersecurity career and technical education (CTE) programs using the NIST National Initiative for Cybersecurity Education (NICE) framework, and the development of a high school apprenticeship program in cybersecurity. The OEA grant had a multiplier effect by building upon and expanding existing work in Colorado Springs to support the cybersecurity and DoD community.

Resiliency Impacts

Increasing Awareness of the Defense Industrial Base

Asset mapping and ecosystem alignment efforts conducted by the Colorado Springs IR team played a key role in increasing regional awareness of the defense industrial base and the unique challenges facing employers and military installations. Outreach and engagement activities aligned regional priorities regarding cybersecurity towards addressing the workforce needs of DoD installations and contractors.

As part of a cybersecurity ecosystem analysis, the Colorado Springs IR team identified 128 cybersecurity companies in their region, ten of whom only provided cybersecurity goods and services, as a “pure-play” provider. In addition, the analysis identified 37 key assets for cybersecurity providers, including five local NSA Certified Centers of Academic Excellence, three major military computer hubs, five veterans transition programs, and five cybersecurity-specific training organizations. These support assets are all aware of the DoD’s impact on Colorado Springs and their role in supporting the DoD cybersecurity workforce. These companies and assets are all mapped on the Colorado Springs Cybersecurity Ecosystem website, which provides additional information on the impact of cybersecurity on the region’s employment and output. The website additionally hosts information on cybersecurity job openings through an Indeed plug-in, cybersecurity-related events and news, and training and education programs in cybersecurity. Events enabled by Colorado Springs’ networking range from a casual “First Friday” gathering for cybersecurity professionals, to cybersecurity job fairs, grant opportunities, and “Capture-the-Flag,” events, during which cybersecurity students and professionals convene to practice cybersecurity skills. These events provide cybersecurity and DoD officials exposure to one-another, unlocking new opportunities for cooperation through contracts and skills development. The Colorado Springs Cybersecurity Website functions as a central hub for the region’s cybersecurity community.

Further, the Colorado Springs grantee's efforts to increase awareness of the defense community and its needs in the region act as a force multiplier for efforts pre-dating the IR grant. As a result of the grant activities, Colorado Springs officials identified the Pikes Peak Small Business Development Center's cybersecurity awareness workshops and training for small businesses. Other local cybersecurity assets identified during this process include accelerators hosted by Catalyst Campus and Exponential Impact, both of whom provide business services to cybersecurity companies seeking to create or enhance opportunities with the DoD or diversify into commercial markets. These organizations share the work being done by the Colorado Springs grantee and viz-versa, growing the regional cooperative network of cybersecurity resources that touch businesses both engaged in the commercial and government sectors. As an added benefit, and because of the exposure to the DoD, any commercial innovation could benefit DoD lethality.

Enhancing Force Multipliers to Support the Defense Industrial Base

The culmination of the Colorado Springs' asset mapping and ecosystem alignment was the creation of the Cybersecurity Coordinating Committee, with representatives from academia, local government, the military, industry, and non-profit cybersecurity organizations. This Committee formed as a result of recommendations from the Cybersecurity Strategic Plan, with working groups aligned with the identified factors of competition for Colorado Spring's cybersecurity community. The working groups and their chair are as follows:

- Economic Growth & Industry: Rotating industry CEO
- Quality of Life: City of Colorado Spring's Office of Innovation & Sustainability
- Incentives and Investment: Colorado Springs Chamber & EDC
- Workforce Development & Education: PPCC & UCCS
- Defense: Rotating military representative
- Innovation: Exponential Impact Accelerator
- Awareness: National Cybersecurity Center
- Specialization: National Cybersecurity Center

As of writing, seven of the eight working groups have defined goals, with the Defense Working Group still seeking a representative from local military installations. Overall, this committee serves as a liaison between the defense community, cybersecurity industrial base and support assets. Through improving coordination between these organizations, the industrial base and support assets can better adapt to reflect DoD needs with regards to operations and skills, augmenting DoD operations in the region. Improved coordination among the community ensures that education and workforce programs address business needs, growing the cybersecurity sector overall in Colorado Springs.

Commercial Diversification of Defense Companies to Sustain the Industrial Base

The Colorado Springs IR grantee plans to provide a suite of diversification services to at least six Colorado Springs cybersecurity companies. Creating commercial opportunities for defense contractors benefits the DoD by mitigating risk from the impact of changes in defense spending, facilitating the development of company talent pools by creating "clearance-in-waiting" jobs, and can potentially result in new innovations for the DoD. Eligible companies must derive at least a quarter of their revenue from DoD contracts and must be at risk to lose at least 5% of their revenue due to changes in DoD expenditures. Participating companies must have executive participation and provide a 10% match on up to the maximum of $50,000 in services. The grantee is measuring outcomes from their program using new sales; retained sales; new jobs; retained jobs; and new clients served, in addition to examining a company narrative describing the benefits of the program to their business.

The team worked with prime contractors to encourage Tier 2 defense suppliers to apply and has contracted with Simon Everett to provide diversification services. Services are modular and individually priced, meaning that if a company does not require the maximum of $50,000 in services, the Colorado Springs team can select an additional company for assistance. Diversification services for participating companies include the following:

- SWOT Analysis & Action Plan
- Technology Transfer Assessments
- Alternative Futures Workshop (Scenario Planning)
- Strategy Canvas Workshop
- Strategic Market Analysis
- Organizational Consulting Activities

Simon Everett sub-contracted with kglobal and CT Cubed to provide communications strategy development and training, and cybersecurity technical expertise respectively. A key challenge for defense contractors used to government RFPs is developing brand and market strategies that demonstrate their value to potential customers. Similarly, any diversification assistance needs to ensure the companies are identifying commercial markets relevant to their cybersecurity capabilities.

Readiness Impacts

Training and People Support

As a result of OEA funded activities, Pikes Peak Community College received the NSA CAE2Y designation. To meet the requirements of the NSA CAE2Y program, PPCC developed Associate of Applied Sciences programs in Cybersecurity and a dual degree AAS in Computer Networking and Cybersecurity that address 11 components of cybersecurity identified by the NSA and DHS. In the fall of 2018, 125 students enrolled in the Cybersecurity AAS, a number that increased by 200% for Fall 2019. The benefits of the CAE2Y designation not only recognizes PPCC as a leader in cyber security education, but also facilitates articulation to 4 Year CAE universities, and creates opportunities for cybersecurity related funding and collaboration in research. Students from local high school cybersecurity CTE programs receive college credit applicable to the PPCC AAS in cybersecurity. As a result of the grantee's outreach to market this program, the number of high schools with a cybersecurity CTE program grew from one to seven of the 16 regional Pikes Peak high schools. High school students in this program receive a CompTIA Sec+ certification and up to a year's credit towards their AAS. Additionally, the PPCC degree program is developing articulation agreements with local four-year colleges, including cybersecurity programs at Regis University, Colorado State University (CSU) Pueblo, and Colorado Technical University (CTU). PPCC has finalized articulation agreements with several four-year universities including CSU Global, Norwich University, Excelsior, and WGU. Legacy DoD technologies designed without cybersecurity in mind already lack the talent to secure these systems as their lifespan is extended. The growth of a strong cybersecurity talent pool in Colorado Springs provides the necessary workers to support these DoD operations.

The apprenticeship program in development by Pikes Peak Community College adds another workforce development opportunity for students interested in cybersecurity in Colorado Springs. Red Rocks Community College (RRCC), a CAE2Y institution, hosts a cybersecurity apprenticeship with Northrop Grumman. Using relationships developed as a result of asset mapping, the PPCC and RRCC officials identified how to adapt the RRCC apprenticeship program with Northrop Grumman to the Pikes Peak region. RRCC served as a key relationship to help PPCC earn its CAE2Y program as well, a favor PPCC passed to other Colorado Community Colleges. The apprenticeship program serves as an opportunity for students to earn while they train in cybersecurity and wait on their security clearance. Veterans who still hold a security clearance can get back into the workforce while they train in cybersecurity. Furthermore, it builds upon a high school apprenticeship program developed by PPCC using a RAMP Grant from NIST NICE, with participating high schoolers eligible to receive credit towards the AAS in cybersecurity.

A key resource to addressing the workforce needs of cybersecurity providers in the Colorado Springs region is the number of separating military members from local installations. It is estimated that, of the 300 to 500 service members leaving local installations a month, 75% report wanting to stay in Colorado Springs, while only 40% report having local opportunities after their service. The Colorado Springs grantee plan to report aggregate data about the cybersecurity training, certifications, career fields, and clearances of transitioning personnel using information supplied by local installations' transition assistance programs. Former service members often have security clearances sought after by local contractors and go to work in support of the DoD mission after obtaining educational credentials.

A study on the key qualifications found on cybersecurity job postings in the Colorado Springs region found 79% of all postings require a security clearance. A clearance is necessary for an employee to work on DoD contracts, although the study also found a secret clearance can take 234 days to process, and a top-secret clearance 468 days to process, on average. With a processing time of up to two-and-a-half years, cybersecurity companies focusing on DoD contracts have a difficult time recruiting cybersecurity employees with lucrative opportunities in the private sector. This makes identifying commercial opportunities for these companies vital. In addition, the grantee is working to develop a "clearance-in-waiting" program, during which cybersecurity hires across companies waiting on their clearance could cooperate on a pool of unclassified work from participating companies. The development of apprenticeship and internship programs at PPCC has become a focus for a successful "clearance-in-waiting" program. This is helping the effort of allowing students to have their clearances processed while they are working in their cybersecurity program. Upon successful completion of coursework, students will be employable, with a clearance, shortly after they finish their degree.

The project also conducted extensive cross walking of military skills, certifications and contracting requirements to civilian standards. The 300 to 500 military members separating from local DoD installations monthly and 23% of PPCC that are veterans or family of service members, many of whom possess highly sought-after security clearances, represent a key talent pipeline for local cybersecurity providers. The Colorado Springs grantee is working with local installations to receive more information on the occupations of separating service members, in order to help them find work or training opportunities in Colorado Springs. With many former service members staying in the region, the Colorado Springs team developed Army and Air Force Career Profiles for businesses that match service member's military experience and certification with occupations and industry certifications. Military contracts' staffing requirements remained riddling for local cybersecurity contractors, and potential employees, who could not identify if they possessed the necessary qualifications in job postings. To address this need, the grantee developed a crosswalk between DoD 8570 requirements and approved civilian baseline certifications. Increased awareness among cybersecurity contractors regarding the qualifications of former service members and staffing requirements for DoD contracts enables contractors to develop better job postings and fill openings more quickly. With an enhanced ability to target veterans with clearances, DoD contractors can fill key positions supporting DoD operations.

Cybersecurity Preparedness

The DoD has invested heavily in cybersecurity capabilities. But the need goes far beyond the defense sector. As government agencies, corporations, and individuals share more of their sensitive information online – and expose that information to the risk of theft or loss – the demand for cybersecurity products and services will continue to rise. Colorado Springs identified an important pathway to economic diversification in targeting and developing the cybersecurity sector. With OEA funds, the region was able to produce a long-term plan to align stakeholders along strategic goals, tactical actions, and implementation timeline. The Colorado Springs Cybersecurity Strategic Plan includes the following 15 recommendations:

- Establish a coordinating committee
- Develop a brand strategy
- Assist defense companies
- Create specialized tax incentives
- Launch a deal-closing fund
- Train the teachers
- Strengthen research capability
- Launch a developer bootcamp
- Create a cyber summer camp
- Develop apprenticeship program
- Create a Cyber Institute
- Create a clearance-in-waiting track
- Capture transition data
- Launch an awareness initiative

- Formalize specialization

With only 10 of the 128 cybersecurity companies in Colorado Springs operating as “pure-play” in cybersecurity, teaching programmers to secure their code written for DoD operations is critical. A key concern among the cybersecurity community of Colorado Springs is the demand for secure coding by contractors for DoD applications. Programming code written without considering security needs requires eight times the number of hours to secure post-script, as un-secure code must be completely re-designed. Working with 18 defense contractors and four other private companies, the grantee is designing a bootcamp to develop secure coding practices among programmers. While still in development, the initial plan is to provide a program during which students will secure their own code, after identifying its weaknesses and vulnerabilities using a DoD tool. Marketing for the program will be funded by local defense contractors, and the Air Force Academy is looking to spin this boot camp off as a capstone course. With programmers writing secure code that reflects DoD security levels, the DoD will have to spend less money re-securing code and will become less vulnerable to cyber-attack.

In the community, addressing cybersecurity is a key consideration. Pikes Peak Community College is piloting cybersecurity concepts in its Advanced Academic Achievement course (designed to help students be successful in college). PPCC is also in the initial phases of developing an AGS (Associate of General Studies) in Secure Coding. Additionally, high schools in the region are integrating cybersecurity at all levels of their K-12 education as a result of the grant. Colorado Springs is also the only Smart Cities community in the nation considering cybersecurity when developing the network of sensors and web services that will enable the city to utilize digital technology to optimize services and infrastructure.

Colorado Springs is also leveraging an important asset in the region, the National Cybersecurity Center (NCC), funded by the state legislature. The Center, launched in March 2016 serves as an authority on public policy and cyber awareness, job creation, and cyber workforce development This includes developing a program instructing municipal government officials how to secure their systems from cyber-attacks, focusing on simple but effective tactics such as preventing phishing. The NCC has partnered with the University of Colorado-Colorado Springs (UCCS) and supports their initiative to establish a Cyber Institute to expand cybersecurity research and education initiatives. Augmented with an already strong local cyber awareness program by the Pikes Peak SBDC, and a NIST 800-171 compliance program by Manufacturer’s Edge, the Colorado MEP Center, the Colorado Springs grantee is creating a culture of cybersecurity in the region. This ensures that local businesses, including DoD contractors, local government, and the local workforce remain oriented towards the DoD mission of securing our nation’s assets from cyber-attack.

Lessons Learned

Greatest Challenge

Cybersecurity companies in the region compete for the same pool of talented workers, compete for the same DoD contracts, and operate in their own technological stovepipes. These divergent interests made developing cooperative partnerships challenging. Uniting these organizations around the shared mission to build the region’s cybersecurity ecosystem, including education, industry, associations, and government, proved challenging because of sometimes-competing interests. Similarly, local defense installations were reluctant about sharing non-personal information on separating military service members; this has delayed the completion of some project tasks. With improved access to this data, employers and education programs could better target separating service members and identify opportunities to engage them in the cybersecurity pipeline.

Sustainability

The cybersecurity ecosystem and its coordinating assets ensure that components of this project will survive beyond the period of OEA funding. First, Pikes Peak Community College fully intends to maintain its CAE2Y accreditation as a vital training asset for the Colorado Springs cybersecurity community. Second, the ecosystem alignment work resulting in the development of the Cybersecurity Coordinating Committee will continue beyond funding, with the Committee planning to maintain itself as a volunteer organization. The assets identified and brought into the cybersecurity ecosystem will continue beyond funding, with their work already impacted by awareness of the DoD mission and their understanding of a healthy cybersecurity ecosystem's role in supporting the DoD mission. Finally, the state of Colorado remains fully invested in developing its cybersecurity industry, with ongoing appropriations to the National Cybersecurity Center and cybersecurity educational programs at the University of Colorado – Colorado Springs. By focusing the initial work of their project on aligning regional assets to supporting the needs of the DoD's cybersecurity operations, the grantee ensured their impact will continue.