

# Cyber Assistance for Maryland Defense Firms

## Final Program Report

*Period of Performance: March 1, 2021 - November 30, 2022*

US Department of Defense  
Office of Local Defense Community Cooperation

OEA Award Number: ST1435-21-05  
Federal Award Number: HQ00052110011



*Disclaimer: This report was prepared under contract with Maryland MEP, Inc., with financial support from the Office of Local Defense Community Cooperation, Department of Defense. The content reflects the views of Maryland MEP, Inc. and does not necessarily reflect the views of the Office of Local Defense Community Cooperation.*

## Table of Contents

|                                                                     |           |
|---------------------------------------------------------------------|-----------|
| <b>EXECUTIVE SUMMARY .....</b>                                      | <b>3</b>  |
| <b>BACKGROUND .....</b>                                             | <b>4</b>  |
| <b>ABOUT THE MARYLAND MANUFACTURING EXTENSION PARTNERSHIP .....</b> | <b>5</b>  |
| <b>MARYLAND ASSET MAP AND CYBERSECURITY ASSET MAP .....</b>         | <b>6</b>  |
| <i>Maryland Defense Industrial Base.....</i>                        | <i>6</i>  |
| <i>Maryland Cybersecurity Focus.....</i>                            | <i>8</i>  |
| <i>Cybersecurity Subject Matter Expertise.....</i>                  | <i>9</i>  |
| <b>PROGRAM DEVELOPMENT .....</b>                                    | <b>10</b> |
| <i>DFARS 252.204-7012 and the NIST SP 800-171.....</i>              | <i>10</i> |
| <i>Gap Assessment Tool.....</i>                                     | <i>11</i> |
| <i>Cybersecurity Maturity Model Certification (CMMC).....</i>       | <i>12</i> |
| <b>PARTNER DEVELOPMENT.....</b>                                     | <b>13</b> |
| <b>OUTREACH AND EDUCATION .....</b>                                 | <b>15</b> |
| <i>DCAP Events.....</i>                                             | <i>15</i> |
| <b>PATH TO COMPLIANCE .....</b>                                     | <b>18</b> |
| <i>Application.....</i>                                             | <i>18</i> |
| <i>DFARS / NIST SP 800-171 Assessment.....</i>                      | <i>18</i> |
| <i>Cyber Mitigation.....</i>                                        | <i>19</i> |
| <b>KEY FINDINGS.....</b>                                            | <b>20</b> |
| <i>DFARS / NIST SP 800-171 Gap Assessment .....</i>                 | <i>20</i> |
| <i>Compliance Analysis .....</i>                                    | <i>22</i> |
| <i>Cybersecurity Mitigation .....</i>                               | <i>24</i> |
| <i>Remediation Implementation.....</i>                              | <i>26</i> |
| <b>PROGRAM ECONOMIC IMPACT .....</b>                                | <b>28</b> |
| <b>DEFENSE AND CYBERSECURITY LANDSCAPE .....</b>                    | <b>29</b> |
| <b>CONCLUSION.....</b>                                              | <b>30</b> |
| <b>DCAP FINAL REPORT: APPENDIX.....</b>                             | <b>31</b> |

## EXECUTIVE SUMMARY

---

Cybersecurity has become and will continue to be one of the single biggest threats to the defense supply chain in the United States. Technology today continues to advance at a pace that is unmatched in history. Along with this technology, cyber-crime has also become a critical threat to the infrastructure as the number of cyber-criminals, hackers, terrorist organizations and State-sponsored cyber warriors continue to adapt and evolve their tools and methods to gain access to critical information. The cost to combat these threats continues to be a challenge as companies struggle to protect their data, assets and other secure information.

To combat these threats, the Department of Defense (DoD) has taken steps to protect information and intellectual property, with a focus on securing Controlled Unclassified Information (CUI) within the defense supply chain. Through the Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012 and the National Institute for Standards and Technology (NIST) Special Publication (SP) 800-171, the DoD has established a requirement that all defense contractors handling CUI must take adequate steps to protect their information and organization from cyber threats. Initially rolled out in 2017, the cybersecurity requirements have helped raise the level of awareness of cybersecurity and improved the general cyber health of companies who have undertaken steps to comply with the requirements. However, to date small and mid-sized suppliers continue to struggle with the requirements for compliance. While companies are now more aware of the requirements, they still remain unsure of how to address deficiencies and/or implement the necessary controls to ensure protection.

Defense contractors and companies looking to address cybersecurity compliance have shared that the requirements can be confusing, and moreover, it can be costly to mitigate issues and protect data and assets on an ongoing basis. Identifying and providing resources to help these organizations raise the overall level of cybersecurity awareness and improve the overall ability to comply with these requirements is critical to reducing the risks to our defense supply chain.

In support of this, in 2018 the DoD's Office of Local Defense Community Cooperation (OLDCC), formerly Office of Economic Adjustment (OEA), provided the State of Maryland's Department of Commerce with funding to directly educate, assess and support defense contractors in complying with the DFARS clause and the requirements of NIST SP 800-171. Through this funding, the Maryland Manufacturing Extension Partnership (Maryland MEP) created the Maryland Defense Cybersecurity Assistance Program (DCAP), an innovative and unique program created through the partnership of OLDCC, the Maryland Department of Commerce, Maryland MEP, cybersecurity subject matter experts and industry. This program leveraged the wealth of cybersecurity talent and resources available in Maryland along with the input of industry to create a dynamic program that has been able to positively impact the organizations that have received assistance.

Due to the success of the program, OLDCC provided additional funding in 2020 and again in 2021 to continue the mission of providing cybersecurity education, resources and financial assistance to small defense contractors in Maryland. The continuation of the program was crucial in the past year as small businesses anticipate the DoD's shift to the Cybersecurity Maturity Model Certification (CMMC). With CMMC and its third-party assessor implications, small businesses now feel their timeline diminishing for implementing solutions.

The following report reflects the cybersecurity landscape in Maryland, the framework for Maryland's Defense Cybersecurity Assistance Program as well as the results, best practices and lessons learned from the delivery of these resources. The program has been instrumental in improving the overall cybersecurity of defense contractors throughout the State of Maryland and will continue to serve the small businesses navigate upcoming DoD requirements.

## BACKGROUND

---

The DFARS Clause 252.204-7012 outlined a set of guidelines and requirements to improve the level of cybersecurity preparedness and compliance, thereby reducing the risk to critical information within the DoD supply chain. This guideline contained a deadline of December 31, 2017 for any defense contractor dealing with CUI to self-certify that they were compliant with the cybersecurity requirements outlined in the NIST SP 800-171 and provided specific requirements for incident response and reporting.

According to the 2018 Manufacturing Division Study by the National Defense Industry Association, less than 60% of small and mid-sized defense contractors said they read the DFARS that lays out minimum security standards for contractor information systems. Of that 60%, half stated that they found it hard to understand. The survey also noted that most companies underestimate the costs of becoming compliant and had a poor understanding of cybersecurity in general.

In response to the DoD requirement, OLDCC provided funding to the Maryland Department of Commerce and Maryland MEP to develop and deliver a program to support the defense contractor community in understanding, assessing and complying with the requirements of NIST SP 800-171. Through this, Maryland MEP developed the Defense Cybersecurity Assistance Program, a program designed to provide education and technical assistance to help contractors with understanding and assessing compliance. Moreover, the program was designed to provide financial and technical resources to help contractors mitigate issues identified through the assessment process. Due to the success and impact of the program on Maryland companies, as well as the continued need for assistance, OLDCC provided additional funding to continue the program in 2020 and again in 2021.

At the start of the program, many small and mid-sized manufacturers and DoD contractors were aware of the requirements within DFARS 252.204-7012 and the upcoming CMMC requirement but lacked the technical knowledge and/or resources to upgrade systems, infrastructure and documentation to ensure compliance and future success with their eventual certification.

The key objectives of the 2021-2022 DCAP program were as follows:

- Provide cybersecurity and DCAP program education throughout the state of Maryland
- Deliver to participating organization a detailed Gap Assessment against the NIST SP 800-171 requirements and provide funding and technical assistance to address cybersecurity requirements and inadequacies
- Provide lessons learned and key findings back to federal and state stakeholders

## ABOUT THE MARYLAND MANUFACTURING EXTENSION PARTNERSHIP

---

The Maryland Manufacturing Extension Partnership (Maryland MEP) is a non-profit organization funded in partnership through Industry, Federal and State government with a mission of growing manufacturing in the State of Maryland. Serving mostly small- and mid-size manufacturers across all industries, Maryland MEP provides an array of programs and services to help these local companies operate more efficiently, grow profitability and create more jobs and opportunities in Maryland. Additionally, Maryland MEP works closely with the defense industrial base to ensure the short and long-term viability of the defense supply chain, providing services such as diversification, market development, cybersecurity and other initiatives that directly improve the competitiveness of Maryland's numerous defense contractors.

Maryland MEP is part of the MEP National Network and annually serves more than 500 manufacturers across the state, annually generating close to \$500 million in economic impact and creating and/or retaining more than 2,500 jobs. The MEP National Network is a unique public-private partnership that delivers comprehensive, proven solutions to U.S. manufacturers, fueling growth and advancing U.S. manufacturing. Focused on helping small and medium-sized manufacturers generate business results and thrive in today's technology-driven economy, the MEP National Network comprises the National Institute of Standards and Technology's Manufacturing Extension Partnership (NIST MEP), the 51 MEP Centers located in all 50 states and Puerto Rico, and over 1,300 trusted advisors and experts at more than 400 MEP service locations, providing any U.S. manufacturer with access to resources they need to succeed.

**Since 2013, Maryland MEP has generated over \$2.1 Billion in direct manufacturing client impacts and created or retained over 8,000 manufacturing jobs.**

## MARYLAND ASSET MAP AND CYBERSECURITY ASSET MAP

---

### Maryland Defense Industrial Base

Defense is a critical sector for Maryland's economy and is home to 20 Military Facilities, 60 Federal Civilian Agencies and 78 Federal Labs. These installations provide the foundation for an incredibly strong and diverse ecosystem of contractors, suppliers, entrepreneurs and customers that make up Maryland's defense industrial base. Within this community there are more than 10,000 aerospace and defense contractors that provide an array of programs, products and services to support the DoD supply chain.

According to OLDCC's Defense Spending by State, Fiscal Year 2021 report, Maryland ranks 8th in the U.S. for Defense Contract Spending with \$17.9B in defense contracts and \$26.3B in Total Defense Spending. In addition to spending, Defense makes up 5.8% of Maryland's total GDP and 4.7% of the Total U.S. Defense Spending. The charts displayed on page 6 show that Maryland has seen incremental increases to the total contracts awarded year after year.

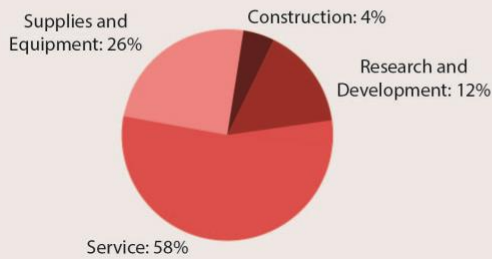
**"Further review shows that some states received substantial funds for both contract and personnel spending, while other states received relatively high amounts in only one. Specifically, California, Florida, Maryland, Texas, and Virginia were all among the top ten recipients of defense contract and personnel spending."\***

In addition, Maryland is proud to be the home to many of the nation's top defense contractors as well as a dense concentration of Military Installations. These organizations support the DoD through research and development, manufacturing and distribution, construction and a variety of other services and support including engineering, software and personnel.

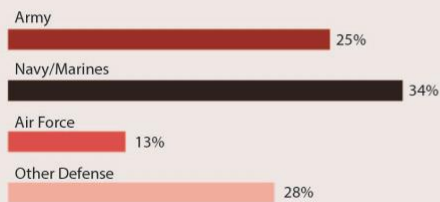
\*[https://oldcc.gov/sites/default/files/OLDCC\\_DSBS\\_FY2021\\_FINAL\\_WEB.pdf](https://oldcc.gov/sites/default/files/OLDCC_DSBS_FY2021_FINAL_WEB.pdf)

## MARYLAND DEFENSE CONTRACTORS

### By Type



### By Service



### Top Defense Contractors (M=millions B=billions)

|                          |           |
|--------------------------|-----------|
| Johns Hopkins University | \$1.6 B   |
| Northrop Grumman         | \$1.3 B   |
| Leidos                   | \$727.3 M |
| Lockheed Martin          | \$705.3 M |
| BAE Systems              | \$534.6 M |
| Booz Allen Hamilton      | \$474.9 M |
| Amentum Services, Inc.   | \$442.1 M |
| Textron                  | \$421.9 M |
| Federal Resources Supply | \$352.6 M |
| General Dynamics         | \$345.0 M |

### Contract Awards Performed (By Fiscal Year, Billions)

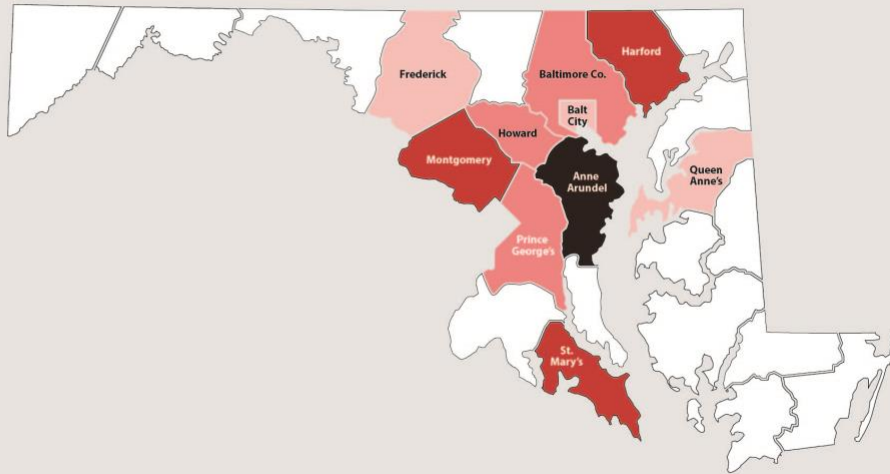


ORIGINAL DATA SOURCE: Office of Local Defense Community Cooperation - Defense Spending by State, FY 2021

ORIGINAL DATA SOURCE: Office of Local Defense Community Cooperation — Defense Spending by State, FY 2021

## TOP DEFENSE CONTRACTOR SPENDING LOCATIONS

|                        |           |
|------------------------|-----------|
| Anne Arundel County    | \$4.3 B   |
| Montgomery County      | \$2.8 B   |
| St. Mary's County      | \$2.6 B   |
| Harford County         | \$2.2 B   |
| Howard County          | \$1.8 B   |
| Baltimore County       | \$1.2 B   |
| Prince George's County | \$1.0 B   |
| Baltimore City         | \$581.8 M |
| Frederick County       | \$513.8 M |
| Queen Anne's County    | \$371.6 M |



ORIGINAL DATA SOURCE: Office of Local Defense Community Cooperation - Defense Spending by State, FY 2021

ORIGINAL DATA SOURCE: Office of Local Defense Community Cooperation — Defense Spending by State, FY 2021

## Maryland Cybersecurity Focus

Maryland's economy is closely tied to the defense sector and with it comes the programs, services and resources required to ensure this defense supply base is strong, resilient and capable of supporting the DoD supply chain today and into the future. In support of this, the State of Maryland has made cybersecurity a primary focus, both in developing cyber organizations, cyber resources and cyber tools, and by also ensuring that these tools and resources are made available to defense contractors and organizations throughout the State that require support.

Maryland is leading the way in creating programs and initiatives to support the development and implementation of cybersecurity for all organizations. In 2018, the Maryland legislature passed the Buy Maryland Cybersecurity Tax Credit, a first-of-its-kind program in the country to provide a tax credit for 50 percent of the purchase price of cybersecurity technologies and services from qualified Maryland companies (with a limit of \$50,000) in tax credits in a single tax year. These tax credits directly benefit small and mid-sized firms that are tackling the DFARS, NIST SP 800-171, and upcoming CMMC requirements to secure their contracts. It also offers a unique benefit for cybersecurity providers in Maryland to gain a competitive advantage by supporting organizations located within the State. DCAP clients with under 50 employees were able to benefit from the program's reimbursement funding and tax credit incentive if they chose to work with one of Maryland's approved cybersecurity providers.

Cybersecurity is a top focus of the Maryland Department of Labor's Employment Advancement Right Now (EARN) program. EARN Maryland is an industry-led initiative that helps businesses cultivate the skilled workforce they need to compete while helping prepare Marylanders find meaningful careers. There are 16 cybersecurity partnerships that have received funding to identify skills gaps and help develop curriculum to address those needs. The required involvement from cybersecurity employers ensures trainees have the skills to meet Maryland cyber employers' tactical and immediate job requirements. In addition to EARN supporting cybersecurity professionals with training, Maryland MEP was awarded EARN funding in 2022 to support cybersecurity training efforts for Maryland's manufacturing and defense firms.

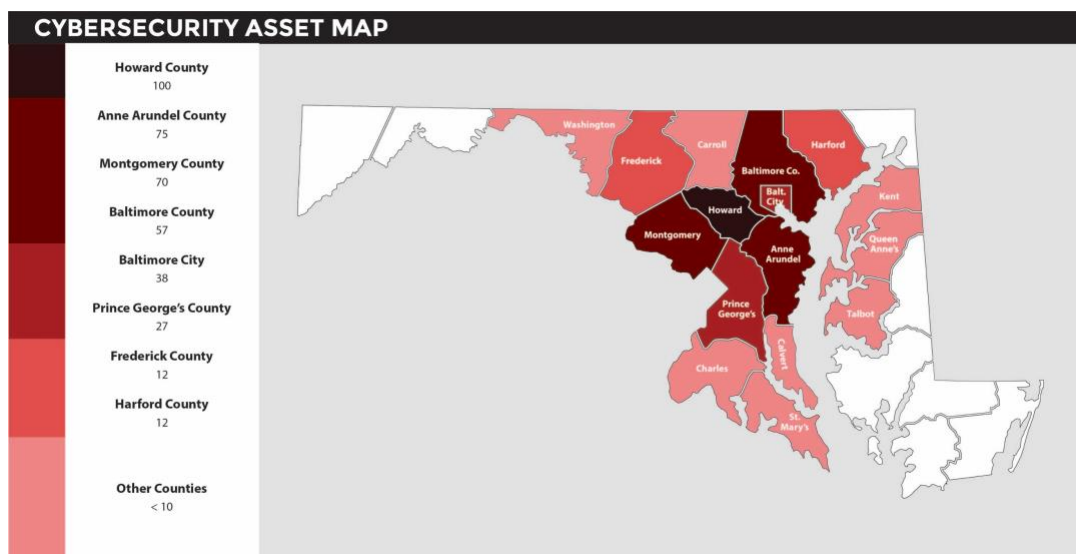
The OLDCC has funded an initiative through University of Maryland, Baltimore County (UMBC) in partnership with Chicago-based MxD (Manufacturing x Digital) to create a robust workforce that has the cybersecurity skills required to assist companies in staying secure in the fast-paced cybersecurity manufacturing industry. MxD is the National Center for Cybersecurity in Manufacturing and focuses on developing new tools to address very specific pain points for manufacturers. It is working with industry and government to figure out how to get these tools to small and medium-sized manufacturers. The partnership between UMBC and MxD, through the OLDCC funding, has developed a curriculum and online platform (<https://cymot.org/>) for manufacturing professionals to increase their cybersecurity skills and to protect manufacturing plants from cyber breaches.

In 2022, Maryland MEP partnered with UMBC to utilize the curriculum and online platform for a brand new Manufacturing Cybersecurity Apprenticeship Program. The program will provide training and skills development to help the Manufacturing IT team to increase their skillset related to cybersecurity with a focus on protecting the operational technology. For manufacturers, protecting the Operational Assets (i.e. CNC Machines, PLCs, MRP) and the software and hardware that actually runs the production lines is critical to the protecting their business. The program will be a combination of classroom, lab and hands-on training which will result in the individual receiving a Registered Apprenticeship Certification as well as solidifying a career path with the manufacturing organization. The Maryland Apprenticeship and Training Council approved the new program in January 2023. Under the new program, Maryland MEP will help clients implement the process, assist with the onboarding of the Registered Apprentice, provide support in the program tracking and reporting and coaching assistance.

Additionally, Maryland’s educational institutions including but not limited to the University of Maryland at College Park, the University of Maryland Baltimore County as well as the robust network of Community Colleges have committed to the development of cybersecurity programs, education and the development of the next generation of cybersecurity professionals. This makes Maryland one of the most resource rich communities for the creation of cybersecurity tools, methods and expertise in the country.

## Cybersecurity Subject Matter Expertise

Maryland’s cybersecurity ecosystem is geographically focused around the large Federal installations including Fort Meade and the National Security Agency and is an environment where cybersecurity providers, contractors and professionals have thrived. It is no surprise that the number of cybersecurity firms and professionals closely mirrors the high density of defense contractor organizations. Maryland is home to over 500 cybersecurity organizations. These companies make up a myriad of service providers, consultants, technical experts, software and hardware developers and other companies committed to the protection of data and information from cyber threats that arise. The diagram below represents a 2019 mapping of the known cybersecurity organizations in Maryland, including their location and density based on contract spending. Through the continued success of the DCAP program and the outreach efforts to the defense community, Maryland MEP was able to identify local and National providers, promote the program and provide access to additional subject matter expertise.

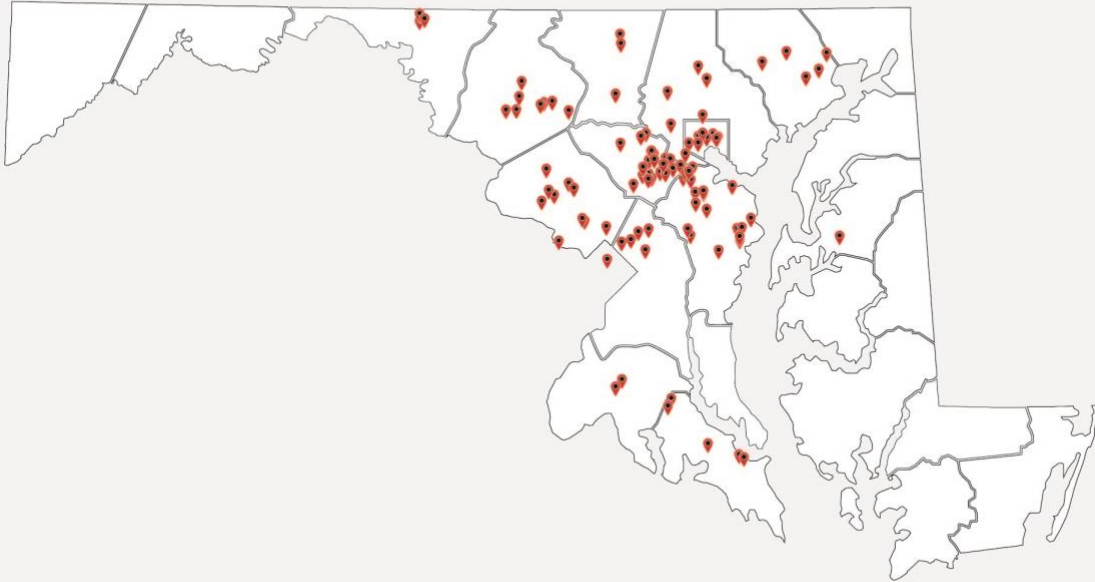


In the development of the DCAP program, Maryland MEP partnered with CAMI for the program launch. Cybersecurity Association of Maryland (CAMI) is the first trade association focused on supporting the cybersecurity professionals and organizations working within the field of cybersecurity. CAMI is a statewide, 501(c)(6) nonprofit organization and is Maryland's only organization dedicated 100% to the growth of Maryland's cybersecurity industry. CAMI hosts a statewide online, searchable directory of hundreds of cybersecurity providers. The partnership led to a sharing of resources and contacts to kick start the partner development needed for DCAP success and identify qualified subject matter experts to support the DCAP initiative.

Since the program inception, the reputation of DCAP has grown, making cybersecurity provider engagement and education a daily occurrence for the Maryland MEP team. To be able to educate more cybersecurity providers than ever before, Maryland MEP recorded an partner event that addressed DCAP past successes, future goals, federal and state stakeholders, and all details pertaining to becoming a DCAP third party provider for Maryland clients.

Through the DCAP 2021-2022 program, Maryland MEP educated an additional 50+ new cybersecurity partners in Maryland and around the country. These partnerships and the partnerships established since 2018 have expanded the reach of the DCAP program to the defense community and has increased the depth of knowledge of services, costs, and alternative solutions for small businesses. Through these partnerships, Maryland MEP has identified and aligned resources across the State to provide services to the contactors that need assistance the most.

## MARYLAND CYBERSECURITY PROVIDER ENGAGEMENT



## PROGRAM DEVELOPMENT

---

### DFARS 252.204-7012 and the NIST SP 800-171

DCAP was designed and developed specifically for Maryland's community of defense contractors that provide products and services to the defense supply chain. The program provides assistance to contractors that are subject to the requirements outlined in the DFARS 252.204-7012 and the NIST SP 800-171. Organized into three key tasks: education, gap analysis and cyber mitigation, DCAP provided financial and technical resources to the defense supplier community to assist with compliance.

NIST published *Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations* in June 2015 (updated January 21, 2016). The purpose of this NIST publication is to provide guidance for federal agencies to ensure that certain types of federal information is protected when processed, stored, and used in non-federal information systems. The NIST SP 800-171 applies to CUI shared by the federal government with a nonfederal entity. In the supply chain context, the federal government often shares data with Original Equipment Manufacturers (OEMs) and/or suppliers for purposes of design, development or manufacturer of products, parts and components utilized in the defense industry. In many of those instances, other federal laws or regulations might address how that information must be protected (e.g., FISMA).

The controls specified in NIST SP 800-171 are based on NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations. The controls were tailored from NIST 800-53 specifically to protect CUI in nonfederal IT systems from an unauthorized disclosure. There are 14 families of security requirements outlined in NIST SP 800-171, comprising 110 individual controls.

The families are:

- Access control
- Awareness and training
- Audit and accountability
- Configuration management
- Identification and authentication
- Incident response
- Maintenance
- Media protection
- Personnel security
- Physical protection
- Risk assessment
- Security assessment
- System and communications protection
- System and information security

Before a company can begin to address the deficiencies within their cybersecurity environment, it is critical that they 1) understand the requirements, the “families” and the controls and 2) have an adequate understanding of not only their current level of compliance but more importantly be able to identify the gaps or areas of risk. DCAP was designed to provide all contractors with a better understanding of NIST SP 800-171 and what compliance meant. All DCAP clients start the program with a DFARS Gap Assessment that mapped all 110 security guidelines outlined in the standard and receive an informed analysis as to whether those requirements were being met.

This assessment serves as the foundation for understanding the current state of each organization, identifying areas of risk and need and providing recommendations and developing a Plan of Action and Milestones (POAM). The 2021-2022 DCAP includes a System Security Plan (SSP) and Vulnerability Scan (optional) to the deliverable items included in the DFARS / NIST SP 800-171 Assessment. Following the DCAP Gap Assessment, clients were able to develop their roadmap and project plan to mitigate outstanding issues and improve their compliance and cybersecurity posture. DCAP provided financial support to offset the cost of remediating gaps within the NIST SP 800-171 requirements. Maryland MEP delivered a DCAP Program info Sheet to provide a summary of the program, deliverables, and the funding available (Appendix A).

## Gap Assessment Tool

In assessing the marketplace, the team identified a wide array of tools, methods and processes to undertake a NIST SP 800-171 gap assessment. The diversity of tools and methods has often created confusion in the market but more importantly it can often create discrepancies in the contractor’s level of “compliance” depending on the answers and documentation provided as well as the thoroughness of the application.

To address this, the DCAP team utilized a common platform known as “FutureFeed” and required all gap assessments be completed within the platform to ensure a common baseline was achieved. By utilizing the same framework of questions for every NIST SP 800-171 gap assessment, the DCAP team was able to ensure consistency across client reviews as well as gain valuable insights into the specific requirements that presented a greater challenge to companies seeking compliance. In addition to providing the common baseline, the FutureFeed platform provided clients with a POAM, SSP, and a dynamic tool for companies to continually update, track and manage their path to compliance.

As a platform, FutureFeed incorporates questions from the *NIST Handbook 162: NIST MEP Cybersecurity Self-Assessment Handbook for Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements*. The addition of this level of detail was crucial to providing guidance for companies and providers as they progressed through the gap analysis.

The FutureFeed platform was utilized again for DCAP 2021-2022 across all clients. The platform has seen increased functionality for clients as they adapt to changes for the Defense community. The platform was updated to calculate the client SPRS score based on the DoD Assessment and Scoring Methodology. Throughout the development of the program, the FutureFeed platform was updated to include key functionality from both a client and provider perspective to ensure that the outcomes met the objectives of the process and the overall program.

In addition, the platform provides the function of organizing POAM items into projects. This provides a tremendous value to the DCAP clients as it simplifies the mitigation process and organizes POAM items into achievable tasks. The enhanced platform allows DCAP clients the ability to assign compliance responsibilities to company users and set established time-based milestone goals as they work towards the 110 SPRS score. These capabilities drastically reduced the consulting cost to prepare these items for the clients and provided a mechanism for the client to continually update as they move toward an eventual CMMC Certification in the future.

## Cybersecurity Maturity Model Certification (CMMC)

In September 2020, the DoD announced an interim DFARS rule to enhance existing regulations while waiting for the implementation and roll-out of CMMC. Effective December 1, 2020, contractors must now submit a self-assessment into DoD's Supplier Performance Risk System (SPRS) by November 30, 2020 before being able to submit bids for new contracts or to renew existing contracts. DCAP assistance with obtaining a current SPRS score was accomplished through the utilization of FutureFeed across all assessments that calculated the score based upon requirements being met. Scores can range between -203 and 110, and Maryland MEP began to track progress made by comparing pre and post mitigation SPRS scores.

Following the interim rule and at the launch of the 2021-2022 DCAP program, the DoD initiated an internal assessment of CMMC 1.0 implementation that was informed by more than 850 public comments in response to the interim DFARS rule. The review resulted in the next version "CMMC 2.0," which changed the proposed structure of the program, elimination of two out of five certification levels, removal of cumbersome requirements within the CMMC levels, and changes to the self-attestation vs. third-party certification requirement for certain CMMC levels. These changes will aim to be implemented through both the title 32 CFR and title 48 CFR rulemaking processes, but until then all CMMC piloting efforts were suspended and any inclusion of a CMMC requirement in solicitations were removed and would not be approved moving forward.

Given this pause of CMMC efforts during the rulemaking process, CMMC did not impact decisions in the DCAP Program structure or development. These changes were welcome to the small business DoD community handling CUI, as it streamlined the CMMC requirements to match those of NIST SP 800-171 and eliminated additional previously proposed new requirements. This allowed for DCAP participants to remain focused on their current contract requirements and provided assurance that improvements in their SPRS score will better prepare them for CMMC success in the future.

## PARTNER DEVELOPMENT

---

Maryland is home to a large number of world-class cybersecurity and technology organizations that are currently developing and deploying services and solutions to protect our nation's supply chain. Maryland MEP solicited input and feedback from the DoD community to develop a cohort of qualified, flexible providers capable of supporting the contractor community with solutions that was tailored specifically to meet their needs. In 2018, Maryland MEP conducted nearly a dozen cybersecurity stakeholder meetings designed to educate and engage cybersecurity experts and stakeholders capable of providing services to the defense contractors within the State of Maryland as well as gain insight to the price structure of cybersecurity deliverables. Maryland MEP then developed a standardized package and approach for delivery to assist in the cybersecurity compliance efforts and more importantly engaged a core-team of cybersecurity services and solutions providers willing to support the contractor community. For the 2021-2022 Program, Maryland MEP aimed to build upon past DCAP successes and make necessary program improvements of the previous funding years.

In March 2021, Maryland MEP consulted with its most active DCAP providers for feedback on the program price structure, deliverables and process. As a result, Maryland MEP made the decision to have the vulnerability scan of the DCAP Assessment as an optional add-on service for the 2021-2022 Program. This allowed for the scope of the vulnerability scan to be better defined and customized for each client while still offering a financial incentive to incorporate a technical component into the DFARS Gap Assessment. Vulnerability scans can target operating systems, applications running on top of those operating systems, web applications, databases, etc. and the appropriate tools to use for vulnerability scans can vary greatly depending on the target environment. Once the assessor had a better gauge for the technologies within the DCAP participant's environment, and the desired scope of the scan, the assessor was better positioned to identify the type(s) of vulnerability scans and the tools needed to perform such scans.

Following the finalization of program details, Maryland MEP facilitated a virtual cybersecurity partner event on April 14, 2021. The purpose of the event was to recap the successes of the 2019 and 2020 DCAP Programs with the most current DCAP cybersecurity partner team along with partners that have expressed interest in assisting DCAP clients. Maryland MEP also presented changes and updates for the 2021-2022 Program. This event was recorded and accessed by potential cybersecurity providers throughout the 2021-2022 Program to gain insight to the DCAP process and details for partner participation. New partners and providers are selected for the DCAP team through an application process that included past and present performance, pricing consideration, area of expertise and client impact. DCAP remained client-focused and allowed for the client to have the ultimate decision on their assessor, whether they were a known partner to Maryland MEP or not.

The team continued to evolve as providers around the state assisted their clients in utilizing the funding available through the program. And to ensure Maryland MEP remain a trusted resource to the Defense Industrial Base for services and guidance in complying and exceeding the cybersecurity requirements set out by the DOD and CMMC-AB, a DCAP partner review process was utilized to address partner performance through a post assessment survey form (Appendix B). The review process consisted of partner engagement, pricing consideration, client reported impact and satisfaction and DCAP program participation.

The 2021-2022 DCAP program included 17 active providers that assisted clients with DFARS / NIST SP 800-171 Assessments. As referenced on page 7 , many of these core-team partners have become an integral part of the State’s cybersecurity resource pool, with over 70% of completed Assessments being performed by Maryland’s “Buy Maryland Cyber Tax Credit” approved sellers.

## OUTREACH AND EDUCATION

---

One of the primary objectives of DCAP was to raise the level of awareness around cybersecurity and the requirements for defense contractors as well as provide education on the elements of DFARS compliance and the future CMMC process and requirements. In September 2018, Maryland MEP worked with the Department of Commerce and utilized the Maryland Defense Network to identify defense contractors that might be subject to the DFARS and NIST SP 800-171 requirements. Maryland MEP used and continues to use this directory to conduct targeted outreach to these organizations to engage them in the program and include them in educational content invitations. Through these collective efforts, Maryland MEP was able to conduct outreach to more than 1,000 different individuals, organizations and contractors throughout Maryland.

### DCAP Events

One of the biggest challenges and risks to the DoD and the entire defense supply chain is ensuring that all defense contractors and suppliers understand the importance of cybersecurity and specifically the requirements of compliance with DFARS and NIST SP 800-171, along with preparation for CMMC. In support of this, a key objective of the DCAP initiative was to provide education throughout the State of Maryland, delivered through a series of educational events, training and programming designed to increase awareness, provide guidance and demonstrate the importance of compliance to securing the supply chain. In 2021, COVID-19 continued to create a number of challenges in the delivery of in-person education and training, however the partnership led by Maryland MEP was able to deliver these services through a series of webinars and videos designed to provide instruction on general cyber hygiene as well as the specific requirements of DFARS, NIST SP 800-171, and CMMC.

Maryland MEP delivered a number of DCAP educational events through webinar format, educating over 210 attendees. Each event recording was uploaded to the Maryland MEP webinar library. The sessions were designed for defense contractors and included an agenda geared toward providing an overview of cybersecurity, a better understanding of cyber-compliance, the specific requirements of NIST SP 800-171, updates and guidance for CMMC, as well as an overview of the tools and resources to help support efforts towards compliance.

MD MEP Webinar Library: <https://mdmep.org/webinar-library/>

### BUILDING A CYBERSECURITY RESILIENT ENVIRONMENT

*July 15, 2021, Presenting Partner: Ntiva, Lnc.*

The Building a Cybersecurity Resilient Environment Webinar was delivered in partnership with the Maryland Procurement Technical Assistance Center (MD PTAC) and included a discussion surrounding access control in a cloud based world, multi-factor authenticator, working from home considerations, as well as the following:

- Alerting, auditing and logging
  - Alerting for system events
  - Alerting for security events
  - Role of Security Information and Event Management (SIEM)
- Where small and mid-sized businesses struggle to meet DoD cyber requirements
  - Multi-Factor Authentication
  - Identification of protected data

- Microsoft Government Community Cloud High (GCC High) decision making assistance
- Separation of duties
- Vulnerability / patch management

## NAVIGATING CMMC 2.0: WHAT DOES IT MEAN FOR YOU?

*January 27, 2022, Presenting Partners: C3 Integrated Solutions and BDO*

In the fall of 2021, the DoD released its recommendations for the next stage in CMMC compliance, CMMC 2.0. While the changes are welcome news for DoD contractors, many are still unsure exactly what it means for them. Others delayed CMMC in anticipation of future changes, and now must begin the process. In January 2022, Maryland MEP along with our presenting partners discussed the changes with CMMC 2.0 and what defense contractors need to do now, no matter where they were on the journey to CMMC 2.0 compliance. Specifically, this webinar covered:

- The significant changes of CMMC 2.0 and their impact on contractors. Are there different requirements for primes vs. subs? Should the compliance strategy change?
- CUI – what it is, how to know whether you have it, and how to get more information from contract officers
- Document requirements for contractors, POAMs and SPRS scores

## CYBERSECURITY THREATS TO MANUFACTURING: WHY THE OSTRICH APPROACH IS A BAD IDEA

*February 16, 2022, Presenting Partner: Summit Business Technologies*

Cyber incidents have become a major problem for the manufacturing industry, costing an average of \$1.52 million dollars. No company is immune from a potential attack, which means everyone in an organization must play a role in safeguarding assets. Maryland MEP, in partnership with Summit Business Technologies, presented a discussion Cybersecurity Threats in Manufacturing, specifically:

- How the threats get in
- What Cyber criminals are after
- Why are those items specifically targeted, and
- Ways to mitigate the risk and protect the company infrastructure.

## THE ROAD TO CMMC WEBINAR SERIES

In the fall of 2021, the DoD released its recommendations for the next stage in CMMC compliance, CMMC 2.0. While the changes are welcome news for DoD contractors, many are still unsure exactly what it means for them. It can be difficult to understand the technical and practical challenges that DoD contractors will face as they navigate compliance. To better assist Maryland's defense community on the changes and its impact, Maryland MEP and its partners developed a three part webinar series covering a variety of essential cybersecurity topics as it relates to their current DFARS requirements and CMMC update including:

- A clear understanding of CUI data
- Importance and necessity of an organization's policies and procedures
- Best practices for small businesses

- Session 1: A CUI Primer

- *April 5, 2022, Presenting Partner: BDO*

Maryland MEP and BDO's Christina Reynolds discussed the practical and technology implications of working with CUI data and specifically:

- The types and categories of CUI
- Different ways to request clarification about CUI from a Contract Authority
- "Legacy CUI" and why this matters
- What to do if CUI is not labeled/encrypted properly
- How to report an incident
- The difference between Personal Identifiable Information (PII), Protected Health Information (PHI) and their CUI counterparts
- Decontrol, disposition, and sanitization
- Marking and safeguarding

- Session 2: Incident Response Planning

- *April 14, 2022, Presenting Partner: Slate Enclave*

Maryland MEP and Slate Enclave discussed the Incident Response (IR) Plan specifically. Developing an incident response plan along with testing the plan will better arm an organization with its best chance in mitigating the negative impacts of a cyber-attack. The presentation specifically walked through understanding what an IR Plan is for an organization and its role in protecting the business. In addition, the webinar covered:

- Understanding what sections should be included within the IR Plan
- Once the IR Plan has been developed... the next steps are testing the plan

- Session 3: Best Practices & Lessons Learned

- April 21, 2022, Presenting Partner: Kaizen Approach*

- This webinar covered small business best practices and the lessons learned through the DCAP. Maryland MEP and Kaizen Approach discussed the options small businesses should consider and keep in mind on the Road to CMMC, specifically:

- Discussion of CUI location within an organization's environment
- Possibility of isolating CUI in an enclave/system
- Possibility of restricted users with access to CUI
- Cloud Software as a Service (SaaS) solutions
- Managed Service Provider Considerations
- Compliance tools and services that are low cost / free
- IT Infrastructure options and the impact of each

# PATH TO COMPLIANCE

## Application

In an effort to ensure the most effective use of OLDCC and program funding, Maryland MEP implemented an application process to gather basic company information as well as verify that the company operates within the defense supply chain and has a need to comply with the cybersecurity requirements. All interested companies were required to submit a DCAP application. Additionally, companies were requested to demonstrate a physical presence in Maryland as well as a minimum of 10% defense dependent business.

## DFARS / NIST SP 800-171 Assessment

Understanding the “current state” of compliance within an organization continued to be the first step in delivery of the program. The DFARS / NIST SP 800-171 Gap Assessment determined the baseline level of compliance, the client’s SPRS score for submission, identified risks or areas of need and developed a Plan of Action and Milestones (POAM) and System Security Plan (SSP) to achieve compliance moving forward. In an effort to ensure DCAP was flexible and capable of meeting the needs of defense contractors of different sizes, the program was designed with a standard price structure and consistent deliverables. Following the application submission, DCAP clients would choose a provider to assist with the DFARS Assessment (either a self-selected third-party provider or a DCAP partner provider). For these assessments, a price was presented based upon the company size and complexity (number of employees, locations, and users were factors in determining which price range was most appropriate). Under the program, DCAP clients received \$2,500 in funding reimbursement for Gap Assessments.

The DCAP DFARS Assessment deliverables included:

- Assessment Responses – Assessment report generated by the FutureFeed platform
- System Security Plan
- Plan of Action and Milestones
- 1-year subscription to the FutureFeed platform
- Recommendations/Cybersecurity Mitigation Plan on hardware, software, or follow-on services such as remediation, consulting and/or On-Going monitoring
- Vulnerability Scanning Add-On (Optional)
- Guidance on SPRS Submission / CUI Training

## DCAP Gap Assessment Breakdown

|                    |                                                |                                              |
|--------------------|------------------------------------------------|----------------------------------------------|
| <b>57</b>          | <b>\$8,560</b>                                 | <b>\$6,500 - \$16,000</b>                    |
| COMPANIES ASSESSED | AVERAGE ASSESSMENT COST PRIOR TO REIMBURSEMENT | ASSESSMENT COST RANGE PRIOR TO REIMBURSEMENT |

## Cyber Mitigation

Utilizing the Gap Assessment data along with their POAM, companies were able to develop a roadmap and plan to mitigate outstanding issues and improve their overall level of compliance by addressing these items. To ensure that companies took action in implementing recommendations and to improve the overall level of compliance of the DoD supply chain, DCAP provided resources in the form of funding to offset the cost of implementing recommendations as well as technical assistance in the form of expertise, tools and programs to address the cybersecurity requirements.

The cyber mitigation funding reimbursement provided under the program was equal to 60% of the cost with a \$12,000 funding cap per organization.

### Cyber Mitigation Breakdown



## KEY FINDINGS

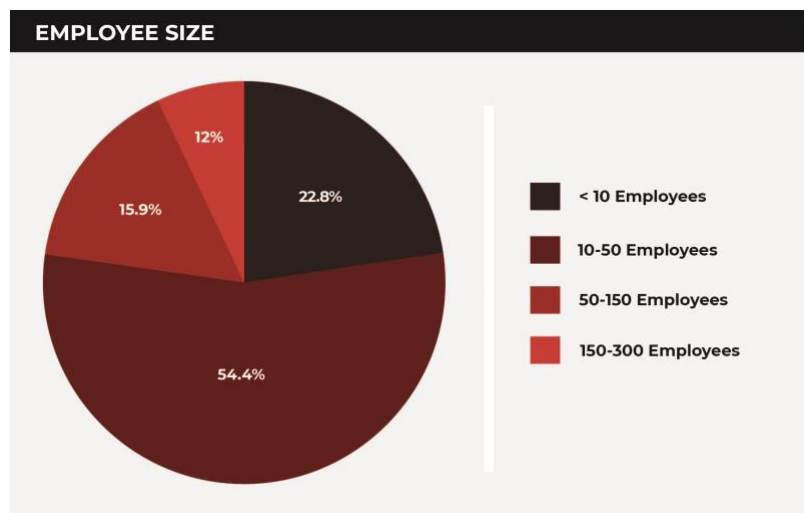
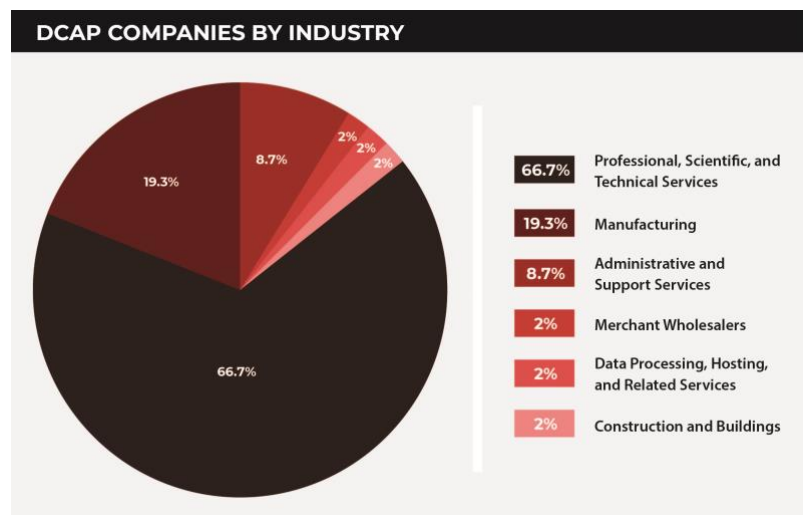
### DFARS / NIST SP 800-171 Gap Assessment

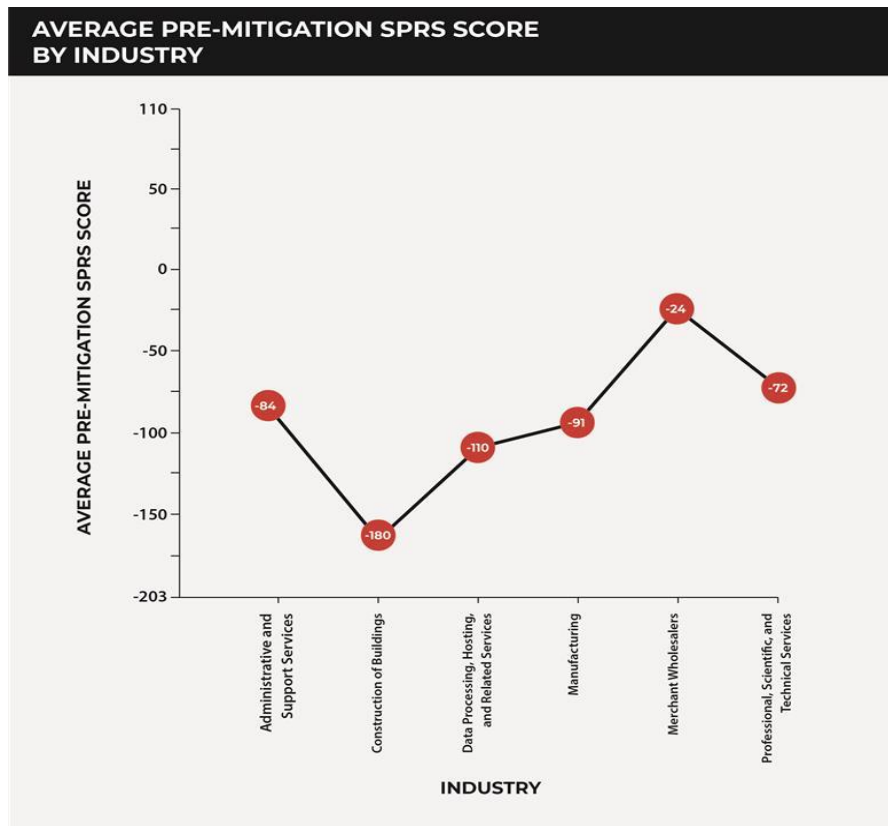
The Maryland DCAP Program is one of the first in the country to provide visibility into the overall level of understanding and compliance with the requirements of DFARS and NIST SP 800-171, and progress made to SPRS scores over time. The point range for an SPRS score is -203 to the highest score of 110, with each of the requirements worth various values (1, 3 or 5). Through the 57 assessments that were performed, the overall average SPRS score was -77. These scores fell in a range from -203 to the highest score of 102. There were no DCAP clients that demonstrated they had already successfully implemented 100% of the requirements.

Additionally, a deeper analysis of the program data revealed information that we believe is critical to securing the overall DoD supply chain. The specific breakdown closely mirrors the population of the Maryland defense industry sectors. The 57 companies that were assessed as part of DCAP represented a diverse group of defense contractors within the following six industry sectors:

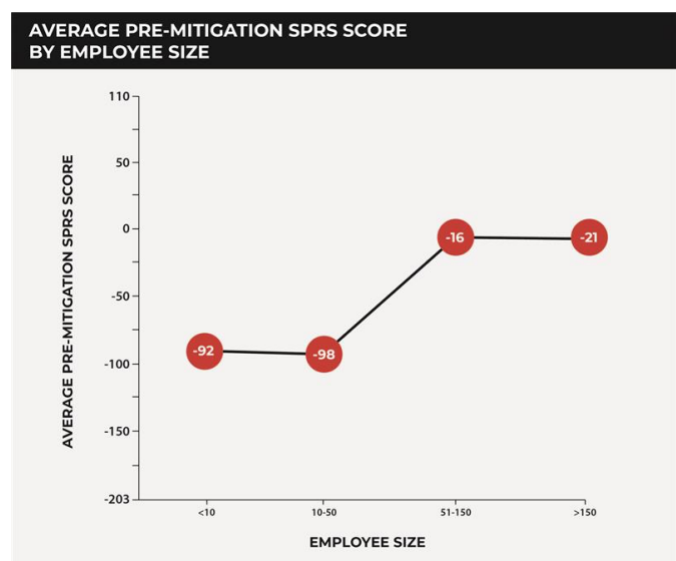
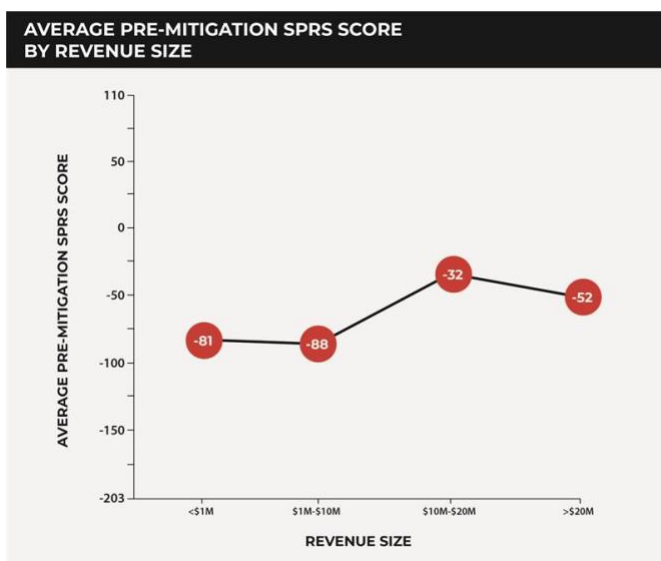
- Professional, Scientific & Technical Services
- Manufacturing
- Administrative & Support Services
- Merchant Wholesalers
- Data Processing, Hosting, and Related Services
- Construction and Buildings

In addition to serving organizations from a variety of industries, DCAP also served a wide range of organizations based on number of employees. This data demonstrates that DCAP provided services to a diverse set of companies and industries within the defense sector. The Average Pre-mitigation SPRS Score by Industry chart (page 20), demonstrates that contractors struggle with compliance regardless of industry or service.





The Assessment data analyses, as indicated in the average pre-mitigation SPRS scores charts below, continue to show a trend that larger size companies, both by employee size and revenue, had more requirements implemented at the time of the initial DCAP Assessment. This can be attributed to larger companies having more fiscal resources as well as acquired internal talent and expertise to begin implementing the requirements. The larger organizations also stressed the influence from their prime contractors to begin implementing solutions prior to entering the DCAP program. The smallest companies struggled the most with the

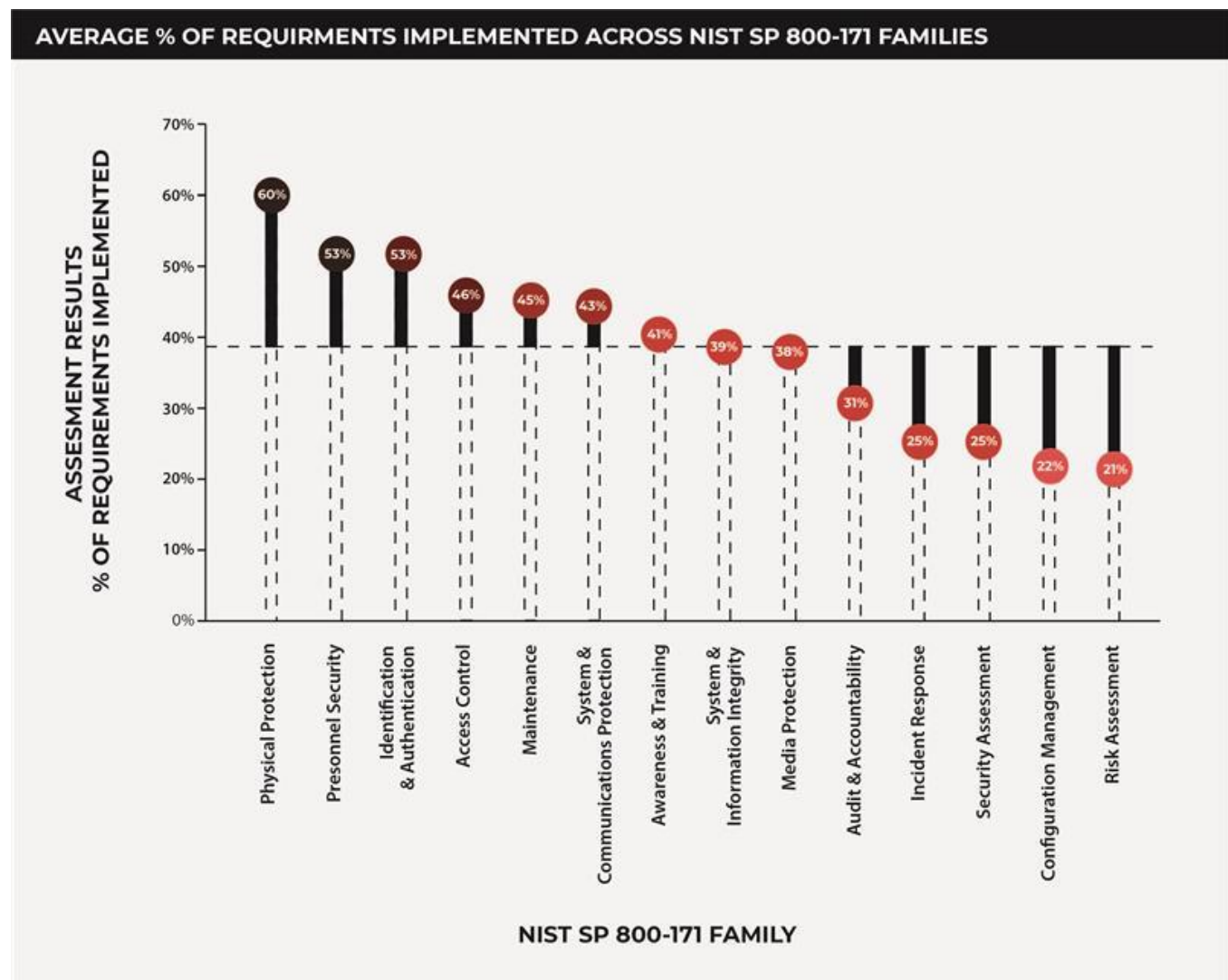


implementation of the NIST SP 800-171 requirements as these companies often lacked technical expertise and financial resources.

## Compliance Analysis

The overall level of compliance with the requirements across the 14 families demonstrated the need for technical assistance and mitigation in ALL areas. A compliance analysis display similarities across the NIST control families, while the individual requirements that were shown to be the least likely to be implemented at the end of the initial Assessment varied from previous DCAP grant periods. 2021-2022 DCAP Assessment results show a trend that the majority of companies are lacking in the areas of assessing and documenting their operational and technical risks, as well as identifying and reporting vulnerabilities and incidents in a timely manner.

Identical to the first and second round of DCAP clients, the Physical and Personnel Security families revealed to be the most implemented family, at an average of between 53-60% of the requirements implemented at the time of the DCAP Gap Assessment, compared to an average of 39% of the requirements implemented across all the Families. And following the trend of the 2018 and 2019 programs, Configuration Management and Risk



Assessment continue to be control families that organizations were lacking solutions. In addition, the Security Assessment and Incident Response families were equally lacking with organizations that were assessed in the 2021-2022 DCAP grant period.

The following thirteen (13) requirements were shown to be the least likely to be fully implemented across all companies.

#### **Access Control**

- 3.1.3: Control the flow of CUI in accordance with approved authorizations.
- 3.1.18: Control connection of mobile devices.

#### **Audit and Accountability**

- 3.3.3: Review and update logged events.
- 3.3.5: Correlate audit record review, analysis, and reporting processes for investigation and response to indication of unlawful, unauthorized, suspicious or unusual activity.

#### **Configuration Management**

- 3.4.2: Establish and enforce security configuration settings for information technology products employed in organizational systems.
- 3.4.7: Restrict, disable or prevent the use of nonessential programs, functions, ports, protocols and services.
- 3.4.8: Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny- all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.
- 3.4.9: Control and monitor user-installed software.

#### **Incident Response**

- 3.6.3: Test the organizational incident response capability.

#### **Risk Assessment**

- 3.11.1: Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.
- 3.11.2: Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

#### **Security Assessment**

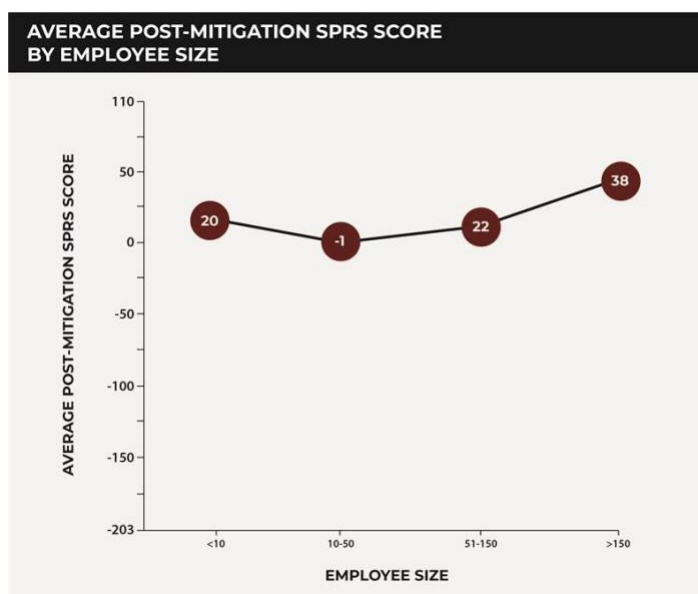
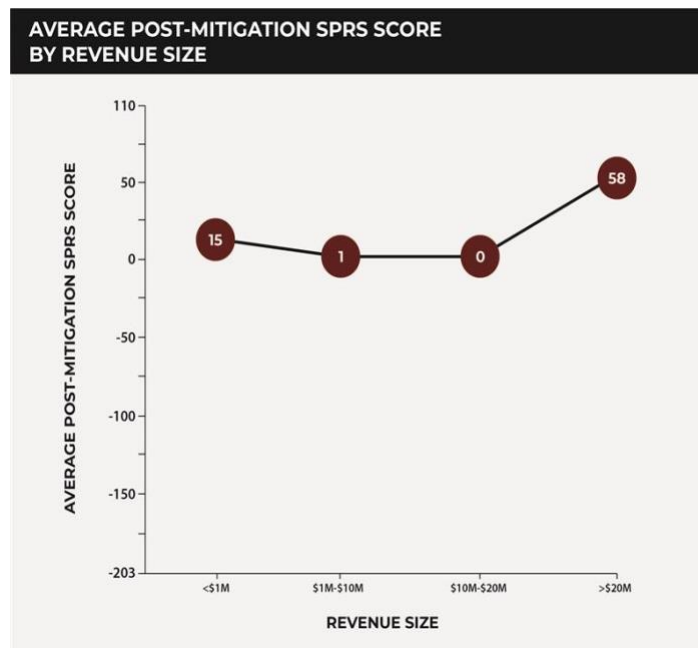
- 3.12.4: Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

#### **Systems and Information**

- 3.14.1: Identify, report, and correct system flaws in a timely manner.

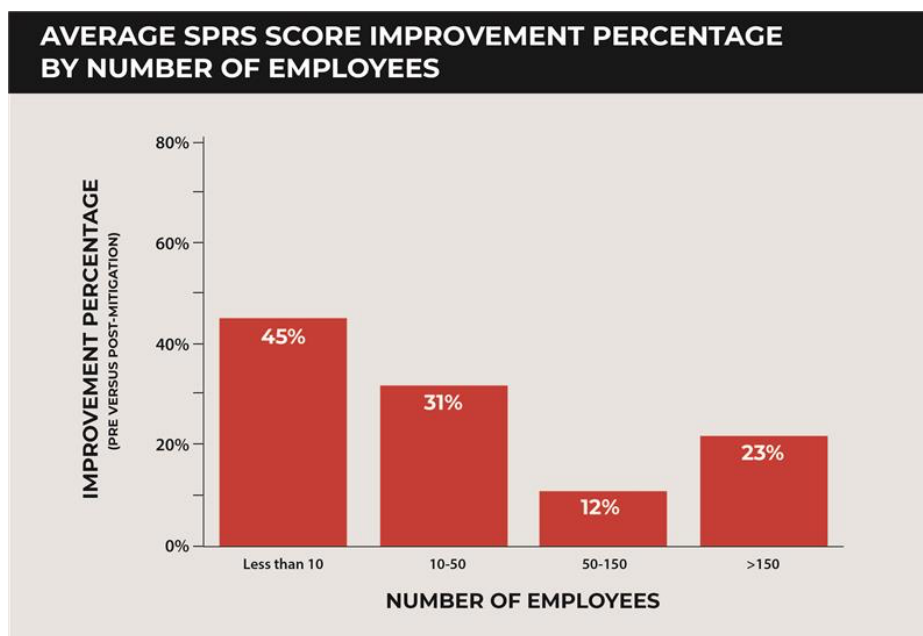
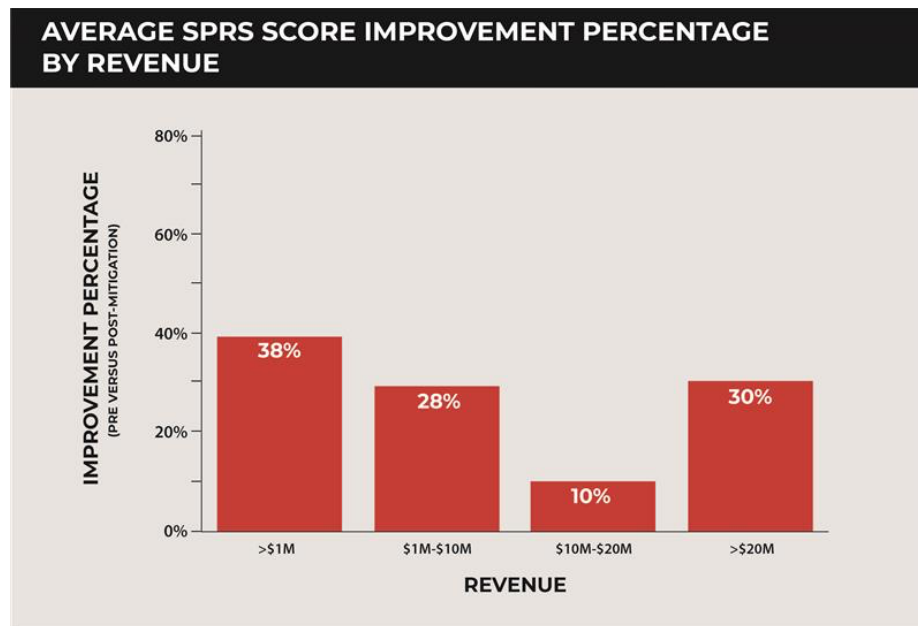
## Cybersecurity Mitigation

Assessment is not enough to ensure compliance with the requirements of NIST SP 800-171 and the eventual CMMC requirement. A core component of DCAP was to provide resources and assistance to companies to mitigate issues identified to increase the cybersecurity posture of DCAP clients. An analysis of the SPRS scores following the completion of their remediation efforts show that on average smaller companies, both by employee size and revenue, maintained a lower SPRS score when compared to larger organizations following their remediation projects. Smaller companies do not have the fiscal resources similar to a larger company and also lack the in-house expertise and time resources to address their POAM projects at the same pace as larger organizations. Smaller organizations also began their DCAP journey with a lower SPRS score prior to completing any remediation efforts.



However, in contrast, smaller organizations witnessed the greatest percentage of improvement from the start of the DCAP program. The comparison between revenue size and employee size as seen in the charts below indicate that employee size plays a larger impact on making compliance gains. The number of users and end points can directly impact the cost of certain mitigation implementation projects, allowing for the substantial 45% improvement in their (organizations with <10 employees) SPRS score and a greater ROI on the grant funding provided to small businesses improvement when comparing percentage improvement of their SPRS score pre- and post-mitigation.

Upon completion of mitigation assistance, the average SPRS score across all organizations improved from -77 to 9, with an average improvement of 29%.



## Remediation Implementation

DCAP companies increased their security posture by implementing solutions and practices to address the 110 NIST SP 800-171 requirements. The projects below are examples of the kinds of remediation projects implemented among DCAP companies and were seen across multiple organizations to address a variety security requirements. Some of the items were purchased and utilized internally or managed through a managed service provider.

### Migration to 365 GCC / GCC High

- Compliance features needed for handling CUI/ITAR data, protecting organizations, and dedicated US infrastructure related to current compliance mandates
- GCC High for ITAR support / Export Controlled Data

### Incident Response Plan and Tabletop Exercises

### Risk Assessment Program

#### Policy and Procedure Assistance

- |                            |                            |
|----------------------------|----------------------------|
| • Data Destruction Policy  | • Antivirus Policy         |
| • Patch Management Policy  | • Physical Security Policy |
| • Website Update Procedure | • Network Security Policy  |
| • Acceptable Use Policy    | • Data Destruction Process |
| • Portal Media Policy      | • Patch Management Process |

### Security Information and Event Management (SIEM) Setup

- Utilize a Security Operations Center (SOC) to send system and device logs to for event correlation and alerting

### Endpoint Protection

- Configure active and periodic malicious code scanning, ensure regular updates are installed to malicious code protection

### Email and Data Security

- Utilize an email security product that performs malicious software scanning, spam detection, and advanced filtering of email communication
- Data Handling, Backup and Restoration

### Group Policy Configurations

- Configure password policies and separate privileged functions with accounts

### Mobile Device Management and Implementation

- Develop policies, procedures, and processes for managing and controlling mobile devices

### Multi-factor Authentication

- Configure multi-factor authentication for privileged accounts, non-privileged accounts, and Virtual Private Network (VPN) access

### Patch Management

- Define and configure a system for patch management of devices and systems

#### **Vulnerability Scanning and Remediation**

- Define a process for completing vulnerability scanning on a periodic basis and remediating discovered vulnerabilities

#### **Strategy Development**

- Develop configuration management policies, procedures, and processes for systems
- Design and implement a backup strategy
- Establish a Training and Awareness Policy and utilize established training vendor
- Onboarding / Offboarding Employee Documentation
- CUI Handling Procedure / CUI Flow Management
- Physical and Facility Security Measures

#### **IT System Access Control**

- Controlling access and monitoring remote connections

## PROGRAM ECONOMIC IMPACT

DCAP was designed with the objective of raising the level of awareness of cybersecurity as well as increasing the overall level of compliance with the cybersecurity requirements of NIST SP 800-171. However, the overall impact of the program is far more important than just the measurement of compliance with the cybersecurity requirements. The contractors served through the program were at risk of losing their existing contracts and sales and more importantly, potentially be prevented from pursuing or obtaining new DoD contracts or sales. In addition, implementing solutions to suffice the cybersecurity requirements can translate into millions of dollars in cost avoidance. DCAP organizations that received remediation funding assistance submitted economic impact surveys that resulted in the following for the 2021-2022 program:



*The retained and increased sales impact translates to greater than a \$1,600: \$1 return on investment for the 2021-2022 DCAP program. In addition to client-reported impact, the DCAP program was able to serve the small business community in Maryland with \$658,000 in direct funding reimbursement.*

The DCAP program since its 2018 inception has generated more than \$2.37 Billion of client reported economic impact that would have been potentially lost and / or realized if the program did not exist. The DCAP program has produced greater than a \$1,100: \$1 return on investment on its combined program funding. Through these contracts retained and/or obtained because of their compliance, DCAP companies were also able to add and retain jobs that specifically relate back to increased DoD contracts as well as add staff to manage contract compliance for their organization. Since 2018, the DCAP has reimbursed Maryland defense contractors over \$1.4M and has generated the following client reported impacts:

### Cumulative Program Impacts



## DEFENSE AND CYBERSECURITY LANDSCAPE

---

The changes and delays to the CMMC program roll out has led to fear and confusion in the defense community as well as a wait and see approach from small businesses. Enforcing the NIST SP 800-171 requirements designed to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) with an audit approach using CMMC 2.0 has been an unpleasant development for defense contractors, particularly small businesses. There is concern that compliance with CMMC 2.0 will reduce small business participation even further, impacting future DoD capabilities. Compliance with CMMC requires time and money, resources that many small companies may not have to spare.

While cybersecurity professionals generally applaud the security controls in the NIST SP 800-171 framework, there are concerns around the implementation of audits and measurements of compliance with the CMMC program in the future. Regardless, experts recommend not waiting and getting started with preparation as this is a process that could take years, not a technical turnkey solution. There are many operational and administrative functions to assess and improve, as well as training within the organization. The current wait and see approach from small businesses could create a surge of demand in the future for compliance assistance once the final rule is announced. The increased demand will continue to create an influx of new cybersecurity providers in the market that see opportunity of selling these now required solutions to small businesses. Misinformation about CMMC is rampant in the IT marketplace and various solutions for NIST SP 800-171 requirements do not have to be expensive. The cost of assessments and mitigation has been steadily increasing and many small and medium sized businesses struggle with finding experienced staff, local expertise they can trust, affordable solutions, as well as the financial resources it takes to implement solutions to ensure they are meeting the security requirements.

## CONCLUSION

---

Maryland MEP is proud to present this report and the findings of the program. Through the support and funding from OLDCC, Maryland MEP and the Maryland Department of Commerce have successfully established the Maryland Defense Cybersecurity Assistance Program as one of the most effective and most impactful programs for cybersecurity within the defense supply chain. The program has been designed, developed and deployed effectively to demonstrate the need for technical and financial assistance for small and mid-sized defense contractors to assist with cybersecurity compliance.

This need has only increased as the DoD continues to move to the Cybersecurity Maturity Certification Model. The cost of cybersecurity expertise continues to increase, negatively impacting small businesses who are struggling to implement the same contract requirements as larger organizations. Implementing practices across these requirements can be a lengthy and cost restrictive process. The DCAP program provided much needed funds for small businesses to assess and mitigate their IT and Cybersecurity controls. The program also enabled small businesses to connect with vetted cybersecurity companies, reinforced the importance of preparation, and provided education/training opportunities to demystify DoD cybersecurity compliance. Most small businesses run their organizations with small margins to have competitive bids for the government acquisitions. DCAP introduced cybersecurity to these organizations and provided a roadmap to closing potential gaps in their security posture – whether in their supply chain or internal business processes.

The defense supply chain is critical to the safety and security of our country, our troops and our intellectual property and it is critical that Maryland and the DoD continues to support efforts to ensure the overall cybersecurity and cyber health of these organizations. Since the program's inception, for every \$1 invested in providing cybersecurity assistance to these organizations more than \$1,100 of economic impact was generated through DCAP.

In an effort to ensure that these resources and support structures are available for the industry stakeholders, MD MEP has undertaken an effort to develop a long-term program strategy to ensure the short-term and long-term sustainability of DCAP and the services provided. Maryland MEP will continue to work closely with partners and stakeholders to develop an ongoing strategy to ensure the sustainability of the program and the continued delivery of DFARS / NIST SP 800-171 assessments and mitigation implementation. The program has developed relationships with cybersecurity experts that serve the small business defense community with low cost / right sized solutions. Maryland MEP aims to identify new sources of funding, develop new cybersecurity marketing materials for the program, and develop new educational training opportunities for the next phase of the program that would attract interest from defense firms. As CMMC requirements evolve and updates for release are announced, MD MEP will continue to keep the community informed of the changes and provide best practices and lessons learned with the roll out of CMMC Certifications.

The defense supply chain remains a key part of Maryland's economy and the results achieved through this program demonstrate the continued need to support this sector.

## DCAP FINAL REPORT: APPENDIX

---

Appendix A: DCAP Program Info Sheet

Appendix B: DCAP Post Assessment Survey

Appendix C: Client and Provider List

Appendix D: Program Financials

## Appendix A: DCAP Program Info Sheet





# MARYLAND DEFENSE CYBERSECURITY ASSISTANCE PROGRAM

### PROGRAM BACKGROUND

Cybersecurity has become and will continue to be one of the single biggest threats to the defense supply chain in the United States. Technology today continues to advance at a pace that is unmatched in history. Along with this technology, cyber-crime has also become a critical threat to the infrastructure as the number of cyber-criminals, hackers, terrorist organizations and State-sponsored cyber warriors continue to adapt and evolve their tools and methods to gain access to critical information. The cost to combat these threats continues to be a challenge as companies struggle to protect their data, assets and other secure information.

To combat these threats, the Department of Defense (DoD) has taken steps to protect Controlled Unclassified Information (CUI) within the defense supply chain. Through the Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012 and the National Institute for Standards and Technology (NIST) Publication 800-171, the DoD has established a requirement that all defense contractors handling CUI must take adequate steps to protect their information and organization from cyber threats. Non-conformance to these cybersecurity requirements could result in loss of contracts.

### ABOUT THE PROGRAM

The Maryland Defense Cybersecurity Assistance Program (DCAP) provides education, resources, funding and assistance for Defense Contractors to comply with the DFARS and NIST 800-171 Standards for cybersecurity, as well as prepare for CMMC. DCAP is funded by Department of Defense's Office of Local Defense Community Cooperation (OLDCC) through the Maryland Department of Commerce and is being coordinated by the Maryland MEP (MD MEP).

### PROGRAM GOALS

- Strengthen Maryland's Defense Supply Chain
- Provide resources for compliance with the DFARS / NIST 800-171 requirements
- Prepare for CMMC Model 2.0 Level 2 Cybersecurity practices

### PROGRAM REQUIREMENTS

- Must be a Defense Contractor with a physical location in Maryland
- 10% or more DoD related business OR a contract/procurement request for compliance

### PROGRAM PROCESS

#### 01 PROGRAM APPLICATION

Please contact MD MEP for the DCAP program application.

#### 02 DFARS/NIST 800-171 ASSESSMENT

Assessment cost is based on the size of company. The Gap Assessment does include the CMMC L3 Requirements

#### 03 OUTCOMES & RECOMMENDATIONS

Compliance Score, Assessment Report, Plan of Action & Milestone (POAM), System Security Plan (SSP), Baseline Vulnerability Scan (optional), Mitigation Recommendations

#### 04 MITIGATE GAPS WITHIN REQUIREMENTS

Funding is available to offset the cost for remediation support, as well as technical assistance.

## DFARS/NIST 800-171 ASSESSMENT

|  Number of Employees |  Cost of Assessment |
|-------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| < 10                                                                                                  | \$6,500                                                                                              |
| 10 - 50                                                                                               | \$9,000                                                                                              |
| 51 - 150                                                                                              | \$11,000                                                                                             |
| 150+                                                                                                  | \$13,000+                                                                                            |

\* Cost subject to change depending on number of locations and complexity of network

### Grant Funding Reimbursement

**\$2,500**

DCAP has funding available to reimburse \$2,500 of the cost for the DFARS/NIST 800-171 Assessment. The Assessment includes: Compliance Score, Assessment Report, Plan of Action & Milestone (POAM), System Security Plan (SSP), Mitigation Recommendations.

Vulnerability Scan Add-on: **\$1,000**

Additional Grant Reimbursement: **\$500**

## MITIGATION

Mitigation needs to be determined by the assessment and level of compliance. Funding may be available to offset the cost of remediation support with a dollar cap per company.

### Grant Funding Reimbursement

**60%**

of the cost of remediation

**UP TO \$12,000**

CONSULTING SERVICES | TOOLS |  
HARDWARE | SOFTWARE

\* Program management fee applies

## PROGRAM IMPACTS

**250** | COMPANIES  
EDUCATED

**80** | CLIENTS  
SERVED

**\$750,000**

DIRECT FINANCIAL  
ASSISTANCE TO CLIENTS

## CLIENT REPORTED IMPACTS

**\$385,949,656**

RETAINED SALES

**\$142,031,669**

INCREASED SALES

**2,318**

RETAINED JOBS

**101**

INCREASED JOBS

**\$1,000 : \$1**

ROI FOR THE OEA AS A RESULT  
OF THE CLIENT REPORTED  
ECONOMIC IMPACT

SARA KEITH

410.733.0219

skeith@mdmep.org

BRANDON CANNADAY

301.254.3280

bcannaday@mdmep.org

## Appendix B: DCAP Post Assessment Survey

---

# DCAP Post Assessment Survey

DFARS 252.204-7012 / NIST 800-171 and CMMC L3



### Survey Respondent

Company Name  
Company Contact

Company Size  
Revenue Size

Assessment Cost  
Funding Amount

Provider Name

INFO@MDMEP.ORG  
443.343.0085  
WWW.MDMEP.ORG  
8894 STANFORD BLVD. SUITE 304  
COLUMBIA, MD 21045

## Assistance with Compliance to DFARS 252.204-7012 / NIST 800-171 and CMMC Prep

Thank you for your participation in the Defense Cybersecurity Assistance Program. We greatly appreciate the time it takes to provide survey responses to the questions below. This survey is used ensure MD MEP remains a trusted resource to the Defense Industrial Base for services and guidance in complying and exceeding the Cybersecurity requirements set out by the DoD and CMMC-AB. The survey also provides MD MEP additional insight into the experience our clients have with our DCAP third-party provider team and is used to make necessary additions and removals from the DCAP Team. Please return the completed form to the MD MEP Cybersecurity Program Manager, Sara Keith, at [skeith@mdmep.org](mailto:skeith@mdmep.org).

1. What were the driving factors that led to you participating in the DCAP Pre-CMMC Level 3 Assessment?
2. Did the MD MEP Team set proper expectations at the onset of the program? If not, please explain.
3. What types of questions were important to you during the vetting process of the DCAP providers?
4. What ultimately made you choose the provider that you did?

## DCAP Post Assessment Survey

Assistance with Compliance to DFARS 252.204-7012 / NIST 800-171 and CMMC Prep



5. What suggestions do you have for the FutureFeed team to increase the end-user experience?

6. On a scale of 1-10, please rate your overall experience with the DCAP provider:

1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☒ 8 ☐ 9 ☐ 10 ☐

7. If you did not rate a 10, what suggestions would you provide? Do you have concerns to share with the MD MEP Team regarding the provider of choice?

8. Do you plan to utilize the same provider for your mitigation efforts?

9. On a scale of 1-10, please rate your experience with the MD MEP Team

1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☒ 8 ☐ 9 ☐ 10 ☐

10. What suggestions do you have for the MD MEP Team to improve the DCAP program process and experience overall?

## Appendix C: Client and Provider List

---

### Assessment Clients

- |                                          |                                     |
|------------------------------------------|-------------------------------------|
| 1. 8-Bit Int, LLC                        | 30. IC-CAP                          |
| 2. ADM Solutions, Inc.                   | 31. In Depth Engineering            |
| 3. Aimcm Consulting, LLC                 | 32. Indian Township Solutions LLC   |
| 4. APS Global                            | 33. iNovex Information Systems      |
| 5. Ascendant Innovations Corp.           | 34. Island Creek                    |
| 6. Aset Partners Corp.                   | 35. Kepora                          |
| 7. AZUSA Solutions                       | 36. KiLee Solutions                 |
| 8. BigBear Analytics                     | 37. Legato LLC                      |
| 9. Bottom Line Technologies              | 38. Marq Solutions, LLC             |
| 10. Caelum Research Corp                 | 39. MASAI Technologies              |
| 11. Callahan Construction Company        | 40. Maven Engineering               |
| 12. Carson Solutions                     | 41. Meggitt Baltimore               |
| 13. Chesapeake Lock & Safe Security      | 42. North American Wave Engine      |
| 14. Chesapeake Machining and Fabrication | 43. Ocean Rider's Engineering       |
| 15. ClearShark                           | 44. Omitron, Inc.                   |
| 16. CMT Services, Inc.                   | 45. Peterson Technologies           |
| 17. Crown Point Technologies             | 46. Precision MicroFab              |
| 18. CS2                                  | 47. Que Technology                  |
| 19. Danko Arlington                      | 48. SageCor Solutions               |
| 20. Datalytica LLC                       | 49. SECO                            |
| 21. Defense Architecture Systems, Inc.   | 50. ServeFed                        |
| 22. Dobbs Defense Solutions              | 51. SiTEC Consulting                |
| 23. DWE                                  | 52. SparkSoft                       |
| 24. Excel Machine and Fabrication        | 53. SSE Solutions, LLC              |
| 25. Falcon Edge Technologies, LLC        | 54. Strategic Engineering Solutions |
| 26. Fuse Engineering                     | 55. Tiber Technologies              |
| 27. G3 Innovative Solutions              | 56. Trinity Technologies            |
| 28. GreyTek                              | 57. Zekiah Technologies             |
| 29. Holmes-Tucker International, Inc.    |                                     |

### Remediation Clients

- |                                    |                                  |
|------------------------------------|----------------------------------|
| 1. AimCM Consulting                | 11. Chesapeake Strategies Group  |
| 2. Aset Partners                   | 12. ClearShark                   |
| 3. AZUSA                           | 13. CMT Services                 |
| 4. Big Bear                        | 14. Crown Point Tech             |
| 5. Bottom Line Technologies        | 15. CS2                          |
| 6. Caelum Research Corporation     | 16. Danko Arlington              |
| 7. Callahan Construction           | 17. Dave Wheatley Enterprises    |
| 8. Carson Solutions                | 18. Defense Architecture Systems |
| 9. Chesapeake Lock & Safe Security | 19. Disk Enterprise Solutions    |
| 10. Chesapeake Machining           | 20. Eureka Strategic             |

- |                                       |                                     |
|---------------------------------------|-------------------------------------|
| 21. Excel Machine & Fabrication       | 35. Meggitt                         |
| 22. Fuse Engineering                  | 36. MIL CORP                        |
| 23. G3 Innovative Solutions           | 37. North American Wave Engine      |
| 24. GreyTek                           | 38. Omitron                         |
| 25. Hamilton Associates               | 39. Que Technology Group            |
| 26. Harry Khan Associates             | 40. Sagecor Solutions               |
| 27. Holmes-Tucker International, Inc. | 41. SECO                            |
| 28. Indian Township                   | 42. ServeFed                        |
| 29. iNovex Information Systems        | 43. SITEC Consulting                |
| 30. Island Creek                      | 44. SSE Solutions                   |
| 31. Kepora                            | 45. Strategic Engineering Solutions |
| 32. Mahlet Consulting                 | 46. Trinity Technology Partners     |
| 33. MASAI                             | 47. WACO Products                   |
| 34. Maven Engineering                 | 48. Zekiah Technologies             |

### Cybersecurity Provider List

1. Braxton-Grant Technologies\*
2. Digital Lantern\*
3. EPOCH\*\*
4. eTrepid\*\*
5. Frontline Managed Services
6. Helm Point Solutions\*
7. HyperVigilance
8. ITSC Secure Solutions, LLC
9. Kaizen Approach\*\*
10. MNS Group\*
11. Ntiva
12. Peerless Tech Solutions\*
13. Ramparts\*\*
14. Slate Enclave\*\*
15. Summit Business Technologies\*\*
16. TCECURE\*\*

\*Maryland Organization

\*\*Maryland Organization + Cybersecurity Tax Credit Approved Seller

## Appendix D: Program Financials

| Maryland MEP, Inc.                                            |                          |                   |                  |                   |                   |                  |                  |                    |                   |                                |
|---------------------------------------------------------------|--------------------------|-------------------|------------------|-------------------|-------------------|------------------|------------------|--------------------|-------------------|--------------------------------|
| Maryland 2021 Defense Cybersecurity Assistance Program (DCAP) |                          |                   |                  |                   |                   |                  |                  |                    |                   |                                |
| Final Program Financial Summary                               |                          |                   |                  |                   |                   |                  |                  |                    |                   |                                |
| As of November 30, 2022                                       |                          |                   |                  |                   |                   |                  |                  |                    |                   |                                |
| Task                                                          | QE 05/31/2021            | QE 08/31/2021     | QE 11/30/2021    | QE 02/28/2022     | QE 05/31/22       | QE 08/31/2022    | QE 11/30/2022    | Total Expenditures | Approved Budget   | Budget less Total Expenditures |
| Task 1 - Program and Partner Development                      | 13,000.00                | 7,000.00          | 5,000.00         | 5,000.00          | 30,000.00         | 15,000.00        | -                | 75,000.00          | 30,000.00         | (45,000.00)                    |
| Task 2 - Education and Outreach                               | -                        | 3,000.00          | -                | 6,000.00          | 9,000.00          | -                | -                | 18,000.00          | 20,000.00         | 2,000.00                       |
| Task 3 - Assessments                                          | 45,500.00                | 66,500.00         | 7,500.00         | 62,500.00         | 17,500.00         | -                | -                | 199,500.00         | 280,000.00        | 80,500.00                      |
| Task 4 - Technical Assistance                                 | 11,160.00                | 63,975.00         | -                | 216,788.00        | 164,476.00        | 36,000.00        | 25,101.00        | 517,500.00         | 500,000.00        | (17,500.00)                    |
| Task 5 - MD MEP Administration & Overhead                     | 20,000.00                | 20,000.00         | 20,000.00        | 20,000.00         | 20,000.00         | 20,000.00        | 20,000.00        | 140,000.00         | 120,000.00        | (20,000.00)                    |
| <b>Total</b>                                                  | <b>89,660.00</b>         | <b>160,475.00</b> | <b>32,500.00</b> | <b>310,288.00</b> | <b>240,976.00</b> | <b>71,000.00</b> | <b>45,101.00</b> | <b>950,000.00</b>  | <b>950,000.00</b> | <b>-</b>                       |
|                                                               |                          |                   |                  |                   |                   |                  |                  |                    |                   |                                |
| <b>Invoicing Schedule</b>                                     | <b>Amount of Invoice</b> |                   |                  |                   |                   |                  |                  |                    |                   |                                |
| QE May 31, 2021 - Dated June 17, 2021                         | \$ 89,660.00             |                   |                  |                   |                   |                  |                  |                    |                   |                                |
| QE Aug 31, 2021 - Dated September 15, 2021                    | \$ 162,500.00            |                   |                  |                   |                   |                  |                  |                    |                   |                                |
| QE Nov 30, 2021 - Dated December 9, 2021                      | \$ 32,500.00             |                   |                  |                   |                   |                  |                  |                    |                   |                                |
| QE Feb 28, 2022 - Dated February 28, 2022                     | \$ 322,600.00            |                   |                  |                   |                   |                  |                  |                    |                   |                                |
| QE May 31, 2022 - Dated May 31, 2022                          | \$ 248,100.00            |                   |                  |                   |                   |                  |                  |                    |                   |                                |
| QE Aug 31, 2022 - Dated September 26, 2022                    | \$ 44,736.00             |                   |                  |                   |                   |                  |                  |                    |                   |                                |
| QE Nov 30, 2022 - Dated December 1, 2022                      | \$ 49,904.00             |                   |                  |                   |                   |                  |                  |                    |                   |                                |
| <b>Total Invoiced to Date</b>                                 | <b>\$ 950,000.00</b>     |                   |                  |                   |                   |                  |                  |                    |                   |                                |

| Task 2 - Workshops |                                                                               |                                                                               |                         |                     |
|--------------------|-------------------------------------------------------------------------------|-------------------------------------------------------------------------------|-------------------------|---------------------|
| QE                 | Activity                                                                      | Description                                                                   | Cost                    | Total Incurred      |
| 8/31/21            | July 15th: Building a Cybersecurity Resilient Environment                     | Building a Cybersecurity Resilient Environment                                | \$ 3,000.00             | \$ 3,000.00         |
| 2/28/22            | January 27th: Navigating CMMC 2.0                                             | Navigating CMMC 2.0: What does it mean for your business?                     | \$ 3,000.00             |                     |
|                    | February 16th: Cybersecurity Threats in Manufacturing                         | Cybersecurity Threats in Manufacturing: Why the Ostrich approach doesn't work | \$ 3,000.00             | \$ 6,000.00         |
| 5/31/22            | April 5th: The Road to CMMC Webinar Series: A CUI Primer                      | A CUI Primer                                                                  | \$ 3,000.00             |                     |
|                    | April 14th: The Road to CMMC Webinar Series: Incident Response Planning 101   | Incident Response Planning 101                                                | \$ 3,000.00             |                     |
|                    | April 21st: The Road to CMMC Webinar Series: Best Practices & Lessons Learned | Best Practices & Lessons Learned                                              | \$ 3,000.00             | \$ 9,000.00         |
|                    |                                                                               |                                                                               |                         |                     |
|                    | <b>Total Incurred</b>                                                         |                                                                               |                         | <b>\$ 18,000.00</b> |
|                    |                                                                               |                                                                               |                         |                     |
|                    |                                                                               |                                                                               | <b>Workshops Budget</b> | <b>\$ 20,000.00</b> |
|                    |                                                                               |                                                                               |                         |                     |
|                    |                                                                               |                                                                               |                         | \$ (2,000.00)       |
|                    |                                                                               |                                                                               |                         |                     |
|                    | <b>NOTES:</b>                                                                 |                                                                               |                         |                     |
|                    | Cyber Workshops / Educational Sessions at Fixed Cost of \$3,000 / Session     |                                                                               |                         |                     |

| Task 3 - DCAP Assessments |                                      |                              |                           |                      |                      |
|---------------------------|--------------------------------------|------------------------------|---------------------------|----------------------|----------------------|
| QE                        | Company                              | DCAP Partner / Assessor      | Company Cost / Cost Share | DCAP Funding         | Total Cost           |
| 5/31/21                   | SECO                                 | Kaizen Approach              | \$ 6,500.00               | \$ 3,500.00          | \$ 10,000.00         |
| 5/31/21                   | SageCor Solutions                    | Kaizen Approach              | \$ 6,500.00               | \$ 3,500.00          | \$ 10,000.00         |
| 5/31/21                   | Tiber Technologies                   | Kaizen Approach              | \$ 6,500.00               | \$ 3,500.00          | \$ 10,000.00         |
| 5/31/21                   | Strategic Engineering Solutions      | Slate Enclave                | \$ 6,500.00               | \$ 3,500.00          | \$ 10,000.00         |
| 5/31/21                   | Precision MicroFab                   | Summit Business Technologies | \$ 4,000.00               | \$ 3,500.00          | \$ 7,500.00          |
| 5/31/21                   | SparkSoft                            | Slate Enclave                | \$ 9,500.00               | \$ 3,500.00          | \$ 13,000.00         |
| 5/31/21                   | Legato LLC                           | Kaizen Approach              | \$ 6,500.00               | \$ 3,500.00          | \$ 10,000.00         |
| 5/31/21                   | Ocean Rider's Engineering            | Kaizen Approach              | \$ 4,000.00               | \$ 3,500.00          | \$ 7,500.00          |
| 5/31/21                   | Peterson Technologies                | EPOCH                        | \$ 6,500.00               | \$ 3,500.00          | \$ 10,000.00         |
| 5/31/21                   | G3 Innovative Solutions              | Summit Business Technologies | \$ 6,500.00               | \$ 3,500.00          | \$ 10,000.00         |
| 5/31/21                   | Chesapeake Lock & Safe Security      | eTrepid                      | \$ 6,500.00               | \$ 3,500.00          | \$ 10,000.00         |
| 5/31/21                   | Maven Engineering                    | Slate Enclave                | \$ 4,000.00               | \$ 3,500.00          | \$ 7,500.00          |
| 5/31/21                   | Trinity Technologies                 | Summit Business Technologies | \$ 4,000.00               | \$ 3,500.00          | \$ 7,500.00          |
| 8/31/21                   | Danko Arlington                      | Peerless Tech Solutions      | \$ 4,000.00               | \$ 3,500.00          | \$ 7,500.00          |
| 8/31/21                   | Fuse Engineering                     | Braxton-Grant Technologies   | \$ 8,500.00               | \$ 3,500.00          | \$ 12,000.00         |
| 8/31/21                   | Bottom Line Technologies             | EPOCH                        | \$ 4,000.00               | \$ 3,500.00          | \$ 7,500.00          |
| 8/31/21                   | iNovex Information Systems           | TCECURE                      | \$ 8,500.00               | \$ 3,500.00          | \$ 12,000.00         |
| 8/31/21                   | Excel Machine and Fabrication        | Peerless Tech Solutions      | \$ 4,000.00               | \$ 3,500.00          | \$ 7,500.00          |
| 8/31/21                   | ClearShark                           | Slate Enclave                | \$ 8,500.00               | \$ 3,500.00          | \$ 12,000.00         |
| 8/31/21                   | DWE                                  | MNS Group                    | \$ 8,500.00               | \$ 3,500.00          | \$ 12,000.00         |
| 8/31/21                   | Zekiah Technologies                  | eTrepid                      | \$ 6,500.00               | \$ 3,500.00          | \$ 10,000.00         |
| 8/31/21                   | Callahan Construction Company        | Helm Point Solutions         | \$ 6,500.00               | \$ 3,500.00          | \$ 10,000.00         |
| 8/31/21                   | Carson Solutions                     | Braxton-Grant Technologies   | \$ 6,500.00               | \$ 3,500.00          | \$ 10,000.00         |
| 8/31/21                   | Kepora                               | Slate Enclave                | \$ 6,500.00               | \$ 3,500.00          | \$ 10,000.00         |
| 8/31/21                   | Dobbs Defense Solutions              | Primvis Inc.                 | \$ 6,500.00               | \$ 3,500.00          | \$ 10,000.00         |
| 8/31/21                   | KiLee Solutions                      | TCECURE                      | \$ 4,000.00               | \$ 3,500.00          | \$ 7,500.00          |
| 8/31/21                   | SiTEC Consulting                     | Summit Business Technologies | \$ 6,500.00               | \$ 3,500.00          | \$ 10,000.00         |
| 8/31/21                   | BigBear Analytics                    | Helm Point Solutions         | \$ 13,500.00              | \$ 3,500.00          | \$ 17,000.00         |
| 8/31/21                   | IC-CAP                               | Kaizen Approach              | \$ 6,500.00               | \$ 3,500.00          | \$ 10,000.00         |
| 8/31/21                   | CS2                                  | EPOCH                        | \$ 6,500.00               | \$ 3,500.00          | \$ 10,000.00         |
| 8/31/21                   | ServeFed                             | Washington Software          | \$ 6,500.00               | \$ 3,500.00          | \$ 10,000.00         |
| 8/31/21                   | APS Global                           | Ramparts                     | \$ 4,000.00               | \$ 3,500.00          | \$ 7,500.00          |
| 11/30/21                  | ServeFed - Vulnerability Scan Add-On | Washington Software          | \$ 1,000.00               | \$ 500.00            | \$ 1,500.00          |
| 11/30/21                  | Caelum Research Corp                 | Ntiva                        | \$ 6,500.00               | \$ 3,500.00          | \$ 10,000.00         |
| 11/30/21                  | North American Wave Engine           | Kaizen Approach              | \$ 4,000.00               | \$ 3,500.00          | \$ 7,500.00          |
| 2/28/22                   | 8-Bit Int, LLC                       | Ramparts                     | \$ 6,500.00               | \$ 3,500.00          | \$ 10,000.00         |
| 2/28/22                   | ADM Solutions, Inc.                  | Kaizen Approach              | \$ 4,000.00               | \$ 3,500.00          | \$ 7,500.00          |
| 2/28/22                   | Aimcm Consulting, LLC                | Etrepid                      | \$ 4,000.00               | \$ 3,500.00          | \$ 7,500.00          |
| 2/28/22                   | Ascendant Innovations Corp.          | Kaizen Approach              | \$ 6,500.00               | \$ 3,500.00          | \$ 10,000.00         |
| 2/28/22                   | Aset Partners Corp.                  | Digital Lantern              | \$ 8,500.00               | \$ 3,500.00          | \$ 12,000.00         |
| 2/28/22                   | CMT Services, Inc.                   | ITSC Secure Solutions, LLC   | \$ 4,000.00               | \$ 3,500.00          | \$ 7,500.00          |
| 2/28/22                   | Crown Point Technologies             | Summit Business Technologies | \$ 4,000.00               | \$ 3,500.00          | \$ 7,500.00          |
| 2/28/22                   | Datalytica LLC                       | Kaizen Approach              | \$ 4,000.00               | \$ 3,500.00          | \$ 7,500.00          |
| 2/28/22                   | Defense Architecture Systems, Inc.   | Peerless Tech Solutions      | \$ 6,500.00               | \$ 3,500.00          | \$ 10,000.00         |
| 2/28/22                   | Falcon Edge Technologies, LLC        | Kaizen Approach              | \$ 4,000.00               | \$ 3,500.00          | \$ 7,500.00          |
| 2/28/22                   | Holmes-Tucker International, Inc.    | eTrepid                      | \$ 10,500.00              | \$ 3,000.00          | \$ 13,500.00         |
| 2/28/22                   | Indian Township Solutions LLC        | Frontline Managed Services   | \$ 6,500.00               | \$ 3,500.00          | \$ 10,000.00         |
| 2/28/22                   | Marq Solutions, LLC                  | Digital Lantern              | \$ 6,500.00               | \$ 3,500.00          | \$ 10,000.00         |
| 2/28/22                   | MASAI Technologies                   | TCECURE                      | \$ 4,000.00               | \$ 3,500.00          | \$ 7,500.00          |
| 2/28/22                   | Meggitt Baltimore                    | Slate Enclave                | \$ 8,500.00               | \$ 3,500.00          | \$ 12,000.00         |
| 2/28/22                   | Omitron, Inc.                        | MNS Group                    | \$ 8,500.00               | \$ 3,500.00          | \$ 12,000.00         |
| 2/28/22                   | SSE Solutions, LLC                   | eTrepid                      | \$ 8,500.00               | \$ 3,500.00          | \$ 12,000.00         |
| 2/28/22                   | Chesapeake Machining and Fabrication | Summit Business Technologies | \$ 6,500.00               | \$ 3,500.00          | \$ 10,000.00         |
| 5/31/22                   | Island Creek                         | TCECURE                      | \$ 6,500.00               | \$ 3,500.00          | \$ 10,000.00         |
| 5/31/22                   | Que Technology                       | Digital Lantern              | \$ 6,500.00               | \$ 3,500.00          | \$ 10,000.00         |
| 5/31/22                   | GreyTek                              | eTrepid                      | \$ 4,000.00               | \$ 3,500.00          | \$ 7,500.00          |
| 5/31/22                   | AZUSA Solutions                      | Kaizen Approach              | \$ 4,000.00               | \$ 3,500.00          | \$ 7,500.00          |
| 5/31/22                   | In Depth Engineering                 | HyperVigilance               | \$ 4,000.00               | \$ 3,500.00          | \$ 7,500.00          |
| <b>Total Incurred</b>     |                                      |                              | <b>\$ 351,500.00</b>      | <b>\$ 199,500.00</b> | <b>\$ 551,000.00</b> |
|                           |                                      |                              | <b>Assessments Budget</b> | <b>\$ 280,000.00</b> |                      |
|                           |                                      |                              |                           | \$ 80,500.00         |                      |

| Task 4 - DCAP Technical Assistance |                                   |                                    |                       |                      |
|------------------------------------|-----------------------------------|------------------------------------|-----------------------|----------------------|
| QE                                 | Company                           | Company Cost / Cost Share          | DCAP Funding          | Total Cost           |
| 5/31/21                            | Mahlet Consulting                 | \$ 7,440.00                        | \$ 11,160.00          | \$ 18,600.00         |
| 8/31/21                            | WACO Products                     | \$ 8,000.00                        | \$ 12,000.00          | \$ 20,000.00         |
| 8/31/21                            | Disk Enterprise Solutions         | \$ 8,000.00                        | \$ 12,000.00          | \$ 20,000.00         |
| 8/31/21                            | Maven Engineering                 | \$ 8,000.00                        | \$ 12,000.00          | \$ 20,000.00         |
| 8/31/21                            | G3 Innovative Solutions           | \$ 8,000.00                        | \$ 12,000.00          | \$ 20,000.00         |
| 8/31/21                            | Excel Machine & Fabrication       | \$ 8,000.00                        | \$ 12,000.00          | \$ 20,000.00         |
| 8/31/21                            | Hamilton Associates               | \$ 2,656.00                        | \$ 3,975.00           | \$ 6,631.00          |
| 2/28/22                            | Callahan Construction             | \$ 8,000.00                        | \$ 12,000.00          | \$ 20,000.00         |
| 2/28/22                            | Carson Solutions                  | \$ 4,496.00                        | \$ 6,744.00           | \$ 11,240.00         |
| 2/28/22                            | Chesapeake Strategies Group       | \$ 5,920.00                        | \$ 8,875.00           | \$ 14,795.00         |
| 2/28/22                            | ClearShark                        | \$ 8,000.00                        | \$ 12,000.00          | \$ 20,000.00         |
| 2/28/22                            | Defense Architecture Systems      | \$ 8,000.00                        | \$ 12,000.00          | \$ 20,000.00         |
| 2/28/22                            | iNovex Information Systems        | \$ 8,000.00                        | \$ 12,000.00          | \$ 20,000.00         |
| 2/28/22                            | North American Wave Engine        | \$ 8,000.00                        | \$ 12,000.00          | \$ 20,000.00         |
| 2/28/22                            | Sagecor Solutions                 | \$ 8,000.00                        | \$ 12,000.00          | \$ 20,000.00         |
| 2/28/22                            | Strategic Engineering Solutions   | \$ 4,415.00                        | \$ 5,125.00           | \$ 9,540.00          |
| 2/28/22                            | Trinity Technology Partners       | \$ 7,956.00                        | \$ 11,900.00          | \$ 19,856.00         |
| 2/28/22                            | Caelum Research Corporation       | \$ 8,000.00                        | \$ 12,000.00          | \$ 20,000.00         |
| 2/28/22                            | Chesapeake Lock & Safe Security   | \$ 8,000.00                        | \$ 12,000.00          | \$ 20,000.00         |
| 2/28/22                            | CS2                               | \$ 8,000.00                        | \$ 12,000.00          | \$ 20,000.00         |
| 2/28/22                            | Dave Wheatley Enterprises         | \$ 8,000.00                        | \$ 12,000.00          | \$ 20,000.00         |
| 2/28/22                            | Danko Arlington                   | \$ 6,899.00                        | \$ 10,347.00          | \$ 17,246.00         |
| 2/28/22                            | Harry Khan Associates             | \$ 8,000.00                        | \$ 12,000.00          | \$ 20,000.00         |
| 2/28/22                            | Holmes-Tucker International, Inc. | \$ 8,000.00                        | \$ 12,000.00          | \$ 20,000.00         |
| 2/28/22                            | ServeFed                          | \$ 8,000.00                        | \$ 12,000.00          | \$ 20,000.00         |
| 2/28/22                            | Zekiah Technologies               | \$ 8,000.00                        | \$ 12,000.00          | \$ 20,000.00         |
| 2/28/22                            | Eureka Strategic                  | \$ 3,866.00                        | \$ 5,797.00           | \$ 9,663.00          |
| 5/31/22                            | SSE Solutions                     | \$ 8,000.00                        | \$ 12,000.00          | \$ 20,000.00         |
| 5/31/22                            | AimCM Consulting                  | \$ 8,000.00                        | \$ 12,000.00          | \$ 20,000.00         |
| 5/31/22                            | MIL CORP                          | \$ 8,400.00                        | \$ 5,600.00           | \$ 14,000.00         |
| 5/31/22                            | Omitron                           | \$ 8,000.00                        | \$ 12,000.00          | \$ 20,000.00         |
| 5/31/22                            | Aset Partners                     | \$ 4,400.00                        | \$ 6,600.00           | \$ 11,000.00         |
| 5/31/22                            | Bottom Line Technologies          | \$ 8,000.00                        | \$ 12,000.00          | \$ 20,000.00         |
| 5/31/22                            | Crown Point Tech                  | \$ 8,000.00                        | \$ 12,000.00          | \$ 20,000.00         |
| 5/31/22                            | Fuse Engineering                  | \$ 8,000.00                        | \$ 12,000.00          | \$ 20,000.00         |
| 5/31/22                            | Kepora                            | \$ 8,000.00                        | \$ 12,000.00          | \$ 20,000.00         |
| 5/31/22                            | MASAI                             | \$ 8,000.00                        | \$ 12,000.00          | \$ 20,000.00         |
| 5/31/22                            | Meggitt                           | \$ 3,000.00                        | \$ 12,000.00          | \$ 15,000.00         |
| 5/31/22                            | Chesapeake Machining              | \$ 6,990.00                        | \$ 10,480.00          | \$ 17,470.00         |
| 5/31/22                            | CMT Services                      | \$ 8,000.00                        | \$ 12,000.00          | \$ 20,000.00         |
| 5/31/22                            | Que Technology Group              | \$ 6,531.00                        | \$ 9,796.00           | \$ 16,327.00         |
| 5/31/22                            | Big Bear                          | \$ 8,000.00                        | \$ 12,000.00          | \$ 20,000.00         |
| 8/31/22                            | Island Creek                      | \$ 8,000.00                        | \$ 12,000.00          | \$ 20,000.00         |
| 8/31/22                            | Indian Township                   | \$ 8,000.00                        | \$ 12,000.00          | \$ 20,000.00         |
| 8/31/22                            | GreyTek                           | \$ 8,000.00                        | \$ 12,000.00          | \$ 20,000.00         |
| 11/30/22                           | AZUSA                             | \$ 2,549.00                        | \$ 3,822.00           | \$ 6,371.00          |
| 11/30/22                           | SITEC Consulting                  | \$ 5,928.00                        | \$ 9,279.00           | \$ 15,207.00         |
| 11/30/22                           | SECO                              | \$ 6,750.00                        | \$ 12,000.00          | \$ 18,750.00         |
|                                    | <b>Total Incurred</b>             | <b>\$ 344,196.00</b>               | <b>\$ 517,500.00</b>  | <b>\$ 861,696.00</b> |
|                                    |                                   |                                    |                       |                      |
|                                    |                                   | <b>Technical Assistance Budget</b> | <b>\$ 500,000.00</b>  |                      |
|                                    |                                   |                                    |                       |                      |
|                                    |                                   |                                    | <b>\$ (17,500.00)</b> |                      |

| Task 5 - Program Administration |                                  |                                                    |              |                      |
|---------------------------------|----------------------------------|----------------------------------------------------|--------------|----------------------|
| QE                              | Activity                         | Description                                        | Cost         | Total Incurred       |
| 5/31/21                         | Quarterly Program Administration | MK 2 days                                          | \$ 3,000.00  |                      |
|                                 |                                  | SK 10 days                                         | \$ 10,000.00 |                      |
|                                 |                                  | SC 2 days                                          | \$ 2,000.00  |                      |
|                                 |                                  | BC 10 days                                         | \$ 5,000.00  | \$ 20,000.00         |
| 8/31/21                         | Quarterly Program Administration | MK 1 days                                          | \$ 1,500.00  |                      |
|                                 |                                  | SK 11 days                                         | \$ 11,000.00 |                      |
|                                 |                                  | SC 2 days                                          | \$ 2,000.00  |                      |
|                                 |                                  | BC 11 days                                         | \$ 5,500.00  | \$ 20,000.00         |
| 11/30/21                        | Quarterly Program Administration | MK 1 days                                          | \$ 1,500.00  |                      |
|                                 |                                  | SK 10 days                                         | \$ 10,000.00 |                      |
|                                 |                                  | SC 2 days                                          | \$ 2,000.00  |                      |
|                                 |                                  | BC 13 days                                         | \$ 6,500.00  | \$ 20,000.00         |
| 2/28/22                         | Quarterly Program Administration | MK 1 days                                          | \$ 1,500.00  |                      |
|                                 |                                  | SK 11 days                                         | \$ 11,000.00 |                      |
|                                 |                                  | SC 2 days                                          | \$ 2,000.00  |                      |
|                                 |                                  | BC 11 days                                         | \$ 5,500.00  |                      |
|                                 |                                  |                                                    |              | \$ 20,000.00         |
| 5/31/22                         | Quarterly Program Administration | MK 1 days                                          | \$ 1,500.00  |                      |
|                                 |                                  | SK 13 days                                         | \$ 13,000.00 |                      |
|                                 |                                  | SC 2 days                                          | \$ 2,000.00  |                      |
|                                 |                                  | BC 7 days                                          | \$ 3,500.00  |                      |
|                                 |                                  |                                                    |              | \$ 20,000.00         |
| 8/31/22                         | Quarterly Program Administration | MK 2 days                                          | \$ 3,000.00  |                      |
|                                 |                                  | SK 14 days                                         | \$ 14,000.00 |                      |
|                                 |                                  | SC 3 days                                          | \$ 3,000.00  |                      |
|                                 |                                  |                                                    |              | \$ 20,000.00         |
| 11/30/22                        | Quarterly Program Administration | SK 17 days                                         | \$ 17,000.00 |                      |
|                                 |                                  | SC 3 days                                          | \$ 3,000.00  |                      |
|                                 |                                  |                                                    |              | \$ 20,000.00         |
|                                 | <b>Total Incurred</b>            |                                                    |              | <b>\$ 140,000.00</b> |
|                                 |                                  | <b>MD MEP Administration &amp; Overhead Budget</b> |              | <b>\$ 120,000.00</b> |
|                                 |                                  |                                                    |              | \$ 20,000.00         |