

# CYBERSECURITY GRANT REPORT

---

Washington State Department of Commerce

Office of Economic Development and Competitiveness

Defense Sector

Contract Number 20-78240-121



## ABOUT IMPACT WASHINGTON

Impact Washington is a non-profit organization that provides competitive, value-driven services. We are the Washington State affiliate of the National Institute of Standards and Technology's Manufacturing Extension Program (NIST MEP).

Since 1997 we have delivered improvement solutions to more than 1,500 Washington State manufacturers.

Our team works to identify the unique challenges and opportunities within companies to make them more profitable and a better workplace. Excellence in manufacturing comes from dedication to leading-edge management and operational practices that keep businesses ahead of the competition.

Our experienced staff is committed to helping build a thriving manufacturing industry across the entire state of Washington by providing a wide array of workplace development, growth, and operational services tailored to small- and medium-sized manufacturers. Our expertise and federal, state, and local resources make improvement, growth, and sustainability possible for manufacturers ready to advance their competitive edge in today's global economy and excel in every facet of manufacturing.

Our focus is always on creating value and strengthening a manufacturer's competitiveness by boosting growth, improving productivity, reducing costs, and increasing capacity through customized, hands-on solutions and implementation.

## CONTACT US

For more information email [info@impactwashington.org](mailto:info@impactwashington.org)  
[www.impactwashington.org](http://www.impactwashington.org)

## AUTHORS

Geoff Lawrence and Carol Blayden, Impact Washington

Kate Kanapeaux, Pacific Northwest Defense Coalition (PNDC)

## CREATIVE

Shayna Sitterud, Lab59

4

EXECUTIVE SUMMARY

5

INTRODUCTION

Purpose and Objectives of Grant  
Contractual Scope of Work

7

DELIVERY METHODOLOGIES

- Cyber Resiliency
- Cyber Independence
  - Outreach
  - Training
  - Supplementary or Alternative Training
  - LMS Cybersecurity Training

12

ENGAGEMENT SUMMARY

16

ENGAGEMENT OUTCOMES

- Cyber Resiliency
  - One-on-One Assessment
- Cyber Independence
  - Awareness Outreach Cadence and Metrics
  - Webinar Topics, Cadence, and Links
  - LMS Training Participation

CONTENTS

25

BUDGET REVIEW

26

NEXT STEPS

27

ACKNOWLEDGMENTS

28

APPENDIX

A. CSP’s RFP Scope of Work	28-34
B. Cybersecurity Service Provider (CSP) Partners participating in Grant	35-37
C. Grant Awardees Company Profiles	38
D. Totem Curriculum	39
E. Detailed Engagement Client Reports	40-53
F. Detailed CSPs report	54-60
G. Outreach Materials	61-66

## EXECUTIVE SUMMARY

In early 2020, Impact Washington (IW) commenced a cybersecurity grant project funded by the Department of Defense Office of Local Defense Community Cooperation (DoD OLDCC) through the Washington State Department of Commerce Office of Economic Development and Competitiveness with the broad intent of strengthening Washington State cybersecurity posture in the defense supply chain. In addition to providing outreach to all known members of the state's defense supply chain on the need for cybersecurity resiliency and providing resource information to improve their cybersecurity understanding and knowledge, cybersecurity assessment and training was provided to over 200 companies and guided expert support was given to 36 individual companies to advance their cybersecurity posture.

Major learnings from the grant project verified that members of the DoD supply chain face considerable roadblocks to pursuing improvement of their cybersecurity posture including fear of unknown costs (>60%), no impending/clear

compliance deadline (>50%), staffing constraints (50%), and no perceived ROI (>20%).

Virtually all individual support recipients expressed that the assistance from cybersecurity professionals was critical to their ability to not only start on their cybersecurity journey, but also to sustain it into the future. They reported that their engagements resulted in a clearer identification of ongoing costs and expenses (hardware, software, software as a service (SaaS), subscriptions, etc.) to achieve and maintain compliance. Participants stated that their general understanding of DoD cybersecurity requirements was significantly elevated and most reported that they felt they had a defined pathway to compliance with DoD cybersecurity standards.

Despite the positive results of the clients' engagement with cybersecurity professionals, most participants expressed ongoing concern about the costs of compliance and staffing to effectuate it.

## INTRODUCTION

### Purpose of Grant

**The purpose of the DoD OLDCC/Commerce grant is captured succinctly in the following grant application narrative:**

*[T]he state of Washington proposes a unique partnership that would strengthen the cybersecurity posture of the state's defense manufacturers by providing awareness, training and proof of fault remediation to [the Washington State defense supply chain]. Through this project, the state will also strengthen its capacity to stimulate cooperation between local/individual and statewide efforts by building partnerships through the MEP and the private sector to enhance relationship development needs that will encourage current and future trust in problem-solving while creating a cost-effective technical assistance delivery model for the DoD that accomplishes their goal of supporting the defense industrial base's cybersecurity resilience.*



### Work Design Under the Grant was Broken Into Two Elements:

#### **CYBER RESILIENCY**

The ability of those in the DoD supply chain to prepare for, respond to, and recover from cyber-attacks.

#### **CYBER INDEPENDENCE**

Outreach and education on cybersecurity risks to DoD supply chain companies and training on best practices, risk mitigation options, and DoD cybersecurity compliance requirements.

## Contractual Scope of Work

### A1. Cyber Resiliency:

Conduct cybersecurity penetration testing, evaluation, and recommendations for correction to a minimum of 1% of the Washington State defense industrial supply chain (19 companies). Follow up with these 19 companies to move the companies from negative resiliency responses to cybersecurity compliance.

### A2. Cyber Independence:

Conduct outreach and education to all 1,900 known defense supply chain companies in the state of Washington with a set goal of training 10% of those companies in the defense industrial supply chain in cybersecurity and resiliency goals under DFAS/DFARS regulations.

## Project background, design, and adaptation from original

Since this grant was written and submitted for approval in mid-2018, numerous changes have occurred in the prevalence and severity of cyber threats and the evolution of DoD cybersecurity compliance requirements, importantly the evolving CMMC (Cybersecurity Maturity Model Certification) standard. In addition, the COVID-19 pandemic significantly changed how the requirements of the grant could be delivered. Appropriate modifications were made to work done to comply with the intent of the grant and its deliverables.



DELIVERY METHODOLOGIES

Following outreach to members of the DoD supply chain in Washington, cybersecurity training and direct support were provided to select clients, as referenced in the grant’s Cyber Resiliency and Cyber Independence elements. Impact Washington utilized several methodologies to reach and support companies:

Cyber Resiliency

The primary focus of cyber resiliency was to assist 19+ members of the Washington State defense supply chain to assess their current level of cybersecurity maturity, provide assistance to advance them toward compliance with DoD cybersecurity requirements (more recently including CMMC), and prepare them to maintain a resilient cybersecurity posture. Though penetration testing was mentioned in the original grant language, through discussions with NIST MEP personnel, sister MEP organizations, and other partners, it was determined early in the grant execution design phase that penetration testing would not be appropriate for companies with a rudimentary cybersecurity posture. Instead, emphasis was placed on supporting select members of the DoD supply chain to move them toward compliance with DoD cybersecurity standards.

There was considerable discussion about how best to provide direct assistance to the DoD supply chain members. In the end, we decided that the best option was to provide support through private companies with expertise and experience in DoD cybersecurity standards. Some of the factors contributing to this determination included:

- It was believed that target companies would need to receive initial support and have an ongoing relationship with an expert cybersecurity resource, so we wanted to facilitate that relationship.
- As there are currently not many cybersecurity practitioners serving the SMB (Small and Medium-sized Business) market, we wanted to spread engagements across several contractors to minimize the influence of a potentially ineffective contractor.
- We wanted to evaluate client receptivity and effectiveness on a variety of support approaches by various contractors.
- Identify the most effective programs to establish replicable support models for other members of the DoD supply chain.

Nine (9) private cybersecurity service providers (CSPs) from a respondent pool of 14 were vetted and contracted to work with clients to provide direct support to selected grantees through an RFP process. (Please see Appendix A for the RFP scope of work and Appendix B for the list of CSPs retained for this grant.) For various reasons, including the competitive nature of the RFP and the opportunity envisaged through the emerging CMMC standard, grant awards were extended to 36 members of the DoD supply chain rather than the 19 stipulated in the grant design. (Please see Appendix C for a complete profile of the 36 businesses who participated in the one-on-one portion of this grant.)

Grant recipients were selected from members of the DoD supply chain applying for consideration through a registration form on the Impact Washington website and publicized through outreach by Impact Washington, public and private partners, and training sessions offered under this grant’s educational cyber independence element. Impact Washington presented grant awards of up to 80% of contract pricing provided by CSPs to companies. A summary of grant awards and total engagement costs follows:

TOTALS	LOW	HIGH	MEAN	MEDIAN
36				
	2	450+	58	
\$592,852	\$6,725	\$40,000	\$16,468	\$12,000
\$323,400	\$5,000	\$28,000	\$8,983	\$7,600
			55%	63%

- CLIENTS SERVED
- COMPANY SIZE (EMPLOYEES)
- ENGAGEMENT COST
- GRANT AWARD
- GRANT AWARD/ENGAGEMENT COST

## Cyber Independence

### Outreach

A listing of the Washington State defense supply chain members was initially compiled with data from grant contractor Community Attributes, Inc. (CAI) of Seattle and presented to Impact Washington for use in the project. The companies identified by CAI were 1,900+ direct contractors to the DoD. However, as there are many additional subcontractors in the supply chain, the CAI list was augmented with other supply chain members provided by Impact Washington's database and partners PNDC (Pacific Northwest Defense Coalition) and Washington PTAC (Procurement Technical Assistance Center). With the addition of these sub-tier suppliers, the final outreach list contained 3,400+ members of the Washington State defense supply chain. Initial outreach consisted of emails to targeted companies, webinar training sessions, and promotion by public and private partners.

### Training

Training is the element that propels companies in the DoD supply chain toward good cyber hygiene and compliance with current DoD standards and prepares them for CMMC audit readiness. The initial grant design envisioned that training would be conducted utilizing five in-person training sessions across Washington. As the grant was initiated just before the beginning of March 2020, when the COVID-19 restrictions started to go into effect, in-person training was not possible. A series of three virtual webinars were planned and delivered in March, April, and August 2020.

Webinar presenters were industry experts who discussed many of the same topics that would have been covered in face-to-face training sessions: the critical need for cybersecurity compliance by members of the defense supply chain; a summary outline of DoD cybersecurity standards and requirements; and various means to undertake work to achieve compliance. All webinars were recorded and have been made available for viewing by interested parties.

These webinars attracted an increasing number of participants as awareness of their occurrence expanded by word-of-mouth and promotion by Impact Washington and its public and private partners.

In May 2021, two “capstone” webinars were conducted for members of the defense supply chain to share experiences and lessons learned from the grant program and to share cybersecurity support resources for future assistance. A specific webinar for partners to support their constituents in their DoD cybersecurity compliance journey took place in June 2021.

When the grant design was in process, it was questionable whether further in-person training sessions could be conducted, so alternative training methods were explored.

### Supplementary or Alternative Training

**The challenge of cybersecurity training is aptly stated below:**

“The Pentagon [has made] big moves in an effort to improve cybersecurity for its industrial base, but so far, the department’s biggest roadblocks early on may be the same confusion, doubt, and uneven compliance from contractors that led to the vulnerabilities in the first place” (Johnson, 2019).

While current DoD and emerging CMMC cybersecurity requirements reflect the DoD’s clear understanding of the need for defense contractors and their supply chains to become compliant, the roadmap for that compliance is less clear. Having shifted the original plan calling for face-to-face seminars, the online training webinars referenced above were organized and conducted. Evaluations were very positive, with ratings from “very good” to “excellent.” However, individual respondents still conveyed some barriers to envisioning and creating a pathway to DoD cybersecurity compliance and future CMMC certification. In discussions with several subject matter expert presenters in the webinars, there was a consensus that events conveying extensive cybersecurity compliance data are likely not the most effective means of providing training for this complex topic. All discussed that better training would be role-based, self-paced, and self-guided, which led several cybersecurity training firms with experience with GRC (Governance, Risk & Compliance) and cybersecurity training via LMS (Learning Management System) platform.

## LMS Cybersecurity Training

One team member with deep expertise in education did a secondary research review in two additional areas:

1. Adult learning theories (andragogy); and
2. Methodologies for teaching cybersecurity to corporate businesses.

LMS platforms represent a cost-effective means of training large numbers of learners and can diminish the perishability of material with the ability to update content as requirements evolve. Select research studies support the best practice of combining cybersecurity training with adult learning theories. Learners have specific, measurable learning outcomes, the ability to select relevant content, access to the material in short, sequential modules, and the ability to track and assess their progress. Overall, when cybersecurity training is grounded in adult learning theories, the activity is more engaging and impactful (Jeffers, 2016).

Findings indicate that LMS CMMC cybersecurity courses can be customized to SMBs with content provided in relatively short ‘small-bite’ segments, accompanied by annotated resources and tips, leading to a clear pathway to certification. Each course would begin with a ‘first phase’ overview of the importance of good cyber hygiene and move into the specific current DoD compliance and future CMMC requirements, with the opportunity for a ‘second phase’ to continue training to become ‘audit-ready.’

Conclusions drawn were that a cybersecurity LMS training platform that incorporates adult learning theories would provide a different, complementary, or alternate approach to in-person events or training webinars. Such an online training course would potentially remove perceived barriers to compliance and enhance each contractor’s view of a pathway to certification. For these reasons, design of an LMS training element was initiated and incorporated into the grant execution plan.

### Some of the features of adopting the LMS training platform into this grant project:

#### Users

- ✓ Multiple role-based users within a single organization, e.g., CEO/Owner, Contract Administration/Legal compliance, IT/Technical
- ✓ Training identified by the user

#### Self-paced

- ✓ Learning modules presented in small, digestible packages by role
- ✓ Guidance to next steps following completion of each module

### Links to the curated body of resources for both practical application and technical support

- ✓ How-to’s with examples, e.g., creating a System Security Plan (SSP)
- ✓ Templates
- ✓ Compliance documents, with updates as they occur
- ✓ List of support resources, e.g., regional technical support partners

#### Trackable

- ✓ Trackable progress of organization and roles within organization by checklist or dashboard
- ✓ Project management feature that assigns appropriate personnel for various implementation responsibilities

### Other features of the LMS platform and resource:

- ✓ A potential tool for prime or upper-tier DoD suppliers to track the progress of sub-tier suppliers
- ✓ Expansion of cybersecurity training beyond DoD supply chain to broader supplier base
- ✓ Integration with Impact Washington Salesforce



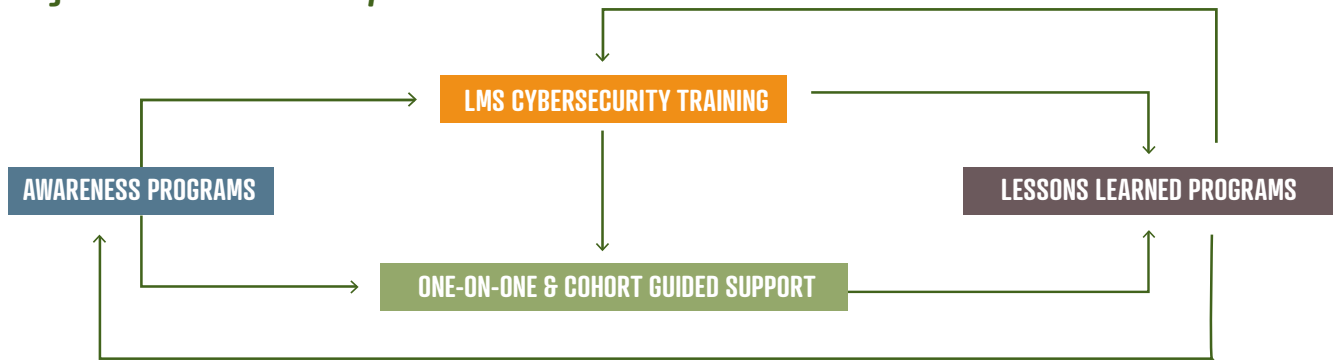
It was envisioned that the online training could be extended and perhaps expanded after the completion of the grant period by subscription of individual contractors, with the support of additional grant(s), or through other funding sources. As CMMC becomes more defined and audits become the norm, prime contractors or upper-tier suppliers in the defense supply chain could potentially utilize resources developed in this project to monitor and track the compliance status of their subs. Additionally, as cybersecurity standards continue to be developed and required beyond the defense supply chain, the resources developed under this grant could be adapted to serve other sectors.

-----

#### References

- Bransford, J. D., Brown, A.L., & Cocking, R.R. (2000) *How People Learn: Brain, Mind, Experience, and School*, Washington, D.C., the National Academy Press.
- Jeffers, T. (2016) *Maximizing Adult Learning Methodologies in Corporate Cybersecurity Training Programs*, Utica College; Retrieved on May 14, 2000, from ProQuest Dissertations.
- Johnson, D.B. (2019, August 12) Contractors have questions about DoD's cyber requirements, FCW the Business of Federal Technology, retrieved on May 15, 2020, from <https://fcw.com/articles/2019/08/12/dod-contractor-cyber-johnson.aspx>
- Knowles, M. (1984) *The Adult Learner: A Neglected Species*, Houston: Gulf Publishing, 3rd edition

## Integrated Look at Delivery



### • AWARENESS PROGRAMS- 3 WEBINARS

Seminars focused on awareness of CMMC requirements and steps needed to become compliant with this emerging requirement. Following the seminars, we asked members of the Washington State Defense Supply Chain what they needed to start or continue their cybersecurity program to meet the CMMC requirements. The below areas were identified and addressed throughout the grant-funded program:

- ✓ Business management (operation, compliance, c-suite) and information technology (IT) in ongoing CMMC programs
- ✓ Support needs vary based on company size, risk exposure, and internal resources available within the business
- ✓ Industry knows WHY they need to be compliant, tell them HOW to achieve compliance
- ✓ Common roadblocks for businesses to begin the compliance process
  - Fear of unknown costs
  - Lack of focused staff time
  - No internal project manager
  - Lack of awareness that all DoD contractors must comply
  - Lack of perceived ROI
  - No impending/clear deadline from DoD

### • LMS CYBERSECURITY TRAINING

Self-paced trainings with tracks for business management and information technology staff provided a deeper understanding of the scope of CMMC to encourage dedication of staff time, budget, and developing a timeline to work toward cybersecurity compliance.

### • ONE-ON-ONE & COHORT GUIDED SUPPORT

Assistance for 36 members of the Washington State defense supply chain with expert technical assistance to create a draft System Security Plan (SSP) and Plan of Action and Milestones (POAM) to assess their current level of cybersecurity maturity and advance towards compliance. Giving a company specific picture of gaps as well as ongoing staff time and budget to maintain the cybersecurity program.

### • LESSONS LEARNED PROGRAMS-3 WEBINARS

Sharing process, results, and referrals to assist others in the Washington State Supply Defense Chain with the CMMC compliance process.

## ENGAGEMENT SUMMARY

### One-on-One and Cohort Guided Support

Under the Cyber Resiliency element of the grant, 36 select members of the Washington State defense supply chain were provided direct support.

Support was provided either with one-on-one engagements between a CSP and the client, or by participation in a cohort model with other clients offered by one of the CSPs. Both delivery methodologies followed the objectives outlined in the project RFP, with the difference in the amount of individual, focused time spent with clients.

Scheduling for one-on-one support was agreed upon between assigned CSPs and their clients, whereas the cohort training and support was delivered in nine (9) 90-minute virtual classroom sessions over three weeks. Please see Appendix D to review the curriculum from Totem.

Tracking and compliance software was included with all engagements. Following is a summary of the breakdown of clients served in one-on-one and cohort engagements:

	ONE-ON-ONE	COHORT
CLIENTS SERVED	26	10
COMPANY SIZE (EMPLOYEES)	29	23
GRANT AWARD - MEDIAN	\$10,000	\$5,000
ENGAGEMENT COST - MEDIAN	\$16,871	\$6,725
GRANT AWARD/ENGAGEMENT COST	59%	74%

### Feedback from the Washington State Defense Supply Chain

In the feedback surveys, members of the 36 Washington State defense supply chain companies that participated in the one-on-one and cohort-guided support/Cyber Resiliency programs provide results of their work with the Cybersecurity Service Providers (CSPs).

86% of participants were satisfied or very satisfied with the work of their CSPs. This exposure to outside cybersecurity support will prove valuable as, according to the post-engagement survey, the majority of companies will continue to outsource all or part of their cybersecurity work.

## Current Plans for Managing Ongoing Cybersecurity\*

When asked to select all that apply from the list below, respondents chose the following:

- 60%** Managed IT Service Provider (outsourced)
- 34%** Managed Cybersecurity Service Provider (outsourced)
- 29%** Full-time IT Staff
- 23%** Part-time IT Staff
- 14%** Part-time Cybersecurity

## Obstacles to Starting the Engagement\*

Respondents indicated the issues they needed to address before engaging with the program:

- 62%** Fear of unknown costs
- 53%** No impending/clear deadline from DoD
- 47%** Lack of focused staff time
- 21%** Lack of perceived ROI
- 15%** No internal project manager
- 3%** Lack of awareness that all DoD contractors must comply

*\* Multiple Choices Allowed*

By the end of the engagement, respondents were asked about additional roadblocks in continuing their cybersecurity journey. A third felt that they had no other roadblocks. Companies that identified challenges focus on a budget (50%) and staff time (40%) as roadblocks to maintain their security program.



### Comments from the Washington State defense supply chain include:

“As a company leader with minimal experience in cybersecurity, we would not be well on our way to CMMC understanding and compliance had Impact Washington not assisted. We would be at high risk of losing our government business, which would have had a catastrophic effect on our company. Thank you, Impact Washington!”

“While we have been impressed with the knowledge the (CSP) team has regarding CMMC

and cybersecurity, we are excited to work with them because they understand that solutions need to be tailored to our business practices rather than another way around. There is still much work to be done for us to reach full compliance with CMMC Level 3 but we are confident that we have chosen the right partner to guide us on this journey.”

“Our prior SPRS score had several unknowns/gaps. The post score was better afterward and had bolstered several areas where we had marginal support.”

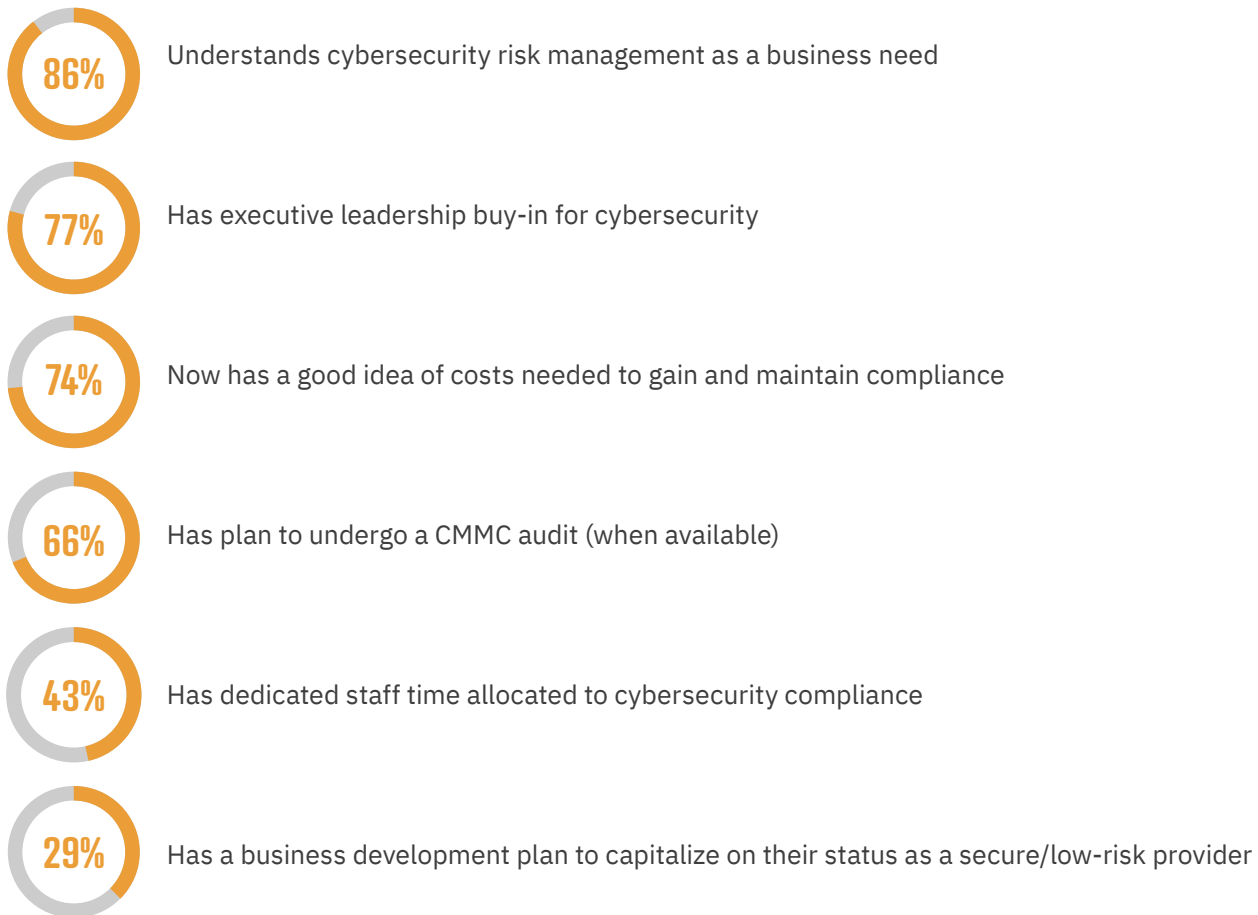
“We look forward to getting to a point where we feel confident using our cybersecurity maturity to market ourselves in proposals. This process has helped set us up to make better the progression needed to get there!”

“This program helps us understand what we need to do to improve our security posture and what an auditor will look for during an audit. This engagement prepares us for our CMMC (audit) later this year.”

## Feedback from Cybersecurity Service Providers:

In feedback surveys, members of the 9 Cybersecurity Service Providers that participated in the Cyber Resiliency program share opinions on their engagement with the Washington State defense supply chain companies. The chart below shows specific results, yet cybersecurity compliance requires continued focus and maintenance. We asked Cybersecurity Service Providers their opinions on the defense supply chain companies' preparedness to maintain focus.

### Opinions at the conclusion of the engagement note that the company:



### Comments from the Cybersecurity Service Providers Include:



“The most valuable aspect of the program was the opportunity to coach, guide, teach, and provide a service to DoD subcontractors in the Defense Industrial Base. Developing relationships with others has also been remarkable. We have met others through some engagements because of this program. It was a great opportunity Providing micro- to small-businesses an extremely low-cost entry point into the DFARS/800-171/CMMC compliance world for everyone to grow and learn.”

COMMENTS



“Continue providing a platform for non-FUD (Fear, Uncertainty, Doubt) pushing consulting firms to get the word out on approachable methodologies for DoD contractor cybersecurity program development. This grant program and the speaking opportunities for companies like Totem have been great.”

“Continue the great work that is—sharing knowledge and spreading awareness by having discussions with local DIBs and providing the DIBs with free training and resources. I do not believe that any DIB is naive enough to say, ‘it won’t happen to us.’ Many in our company are worried that it will happen to us. We are a 20-person shop, and we all wear multiple hats. There is not enough time in the day to accomplish being compliant to CMMC without the assistance of a full-time employee (IT/Compliance) or an outsourced solution.”

“Cybersecurity is an ever-evolving field, and CMMC is, by definition, a framework to improve a company’s cybersecurity environment. We think it is important for companies to realize that different facets are examined when determining a company’s cybersecurity posture. One is business need—without DFARS / CMMC compliance, a company will not provide a product to the DoD. Another is data security and risk management. Cyber espionage and data theft are what nation-state adversaries want, but ransomware has the highest immediate cost. Today, they are interconnected.”

“Impact Washington was a great partner to work with—Geoff and team were clear about deliverables and provided our assessment teams with all the support needed to conduct their assessments.”

# ENGAGEMENT OUTCOMES

## Cyber Resiliency

### One-On-One Assessments

Three benchmarks were used to track the progress of the Washington State Defense Supply Chain Companies’ engagements with the Cybersecurity Service Providers. As each company started with a different cybersecurity posture, their individual progress varied, yet all showed significant improvement.

- ✓ Creation of a System Security Plan (SSP): An overview of the company’s security requirements describing the controls in place or planned, responsibilities and expected behavior of all individuals who access the system.
- ✓ Creation of a Plan of Action and Milestone (POAM): A document that identifies all cybersecurity tasks needed to be accomplished with details on resources required to accomplish, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
- ✓ Increase in the Supplier Performance Risk System (SPRS) cybersecurity score, a performance information assessments site for the Department of Defense acquisition community to use in identifying, assessing, and monitoring unclassified performance.

Please see Appendix E for detailed engagement reports from clients served, and Appendix F for detailed CSPs reports.

### Average SPRS Score Increase - 50

#### Company’s System Security Plan (SSP) status



#### Plan of Action and Milestone (POAM) Status



## Cyber Indpendence

### Awareness-Outreach Cadence and Metrics

The success of outreach efforts was measured using metrics available through the Impact Washington VSM website platform. The Impact Washington team was able to gauge the effectiveness of which emails reached the target audience and the extent to which recipients engaged with the content.

#### The core metrics that supported the analysis are defined below:

- ✓ Delivery rate: Percentage of total emails sent that were delivered successfully
- ✓ Unique open rate: Percentage of successfully delivered emails that are opened at least once
- ✓ Unique click-through rate: Percentage of unique opens that result in at least one click on a link

These metrics were supplemented with data collected through Google Analytics, capturing traffic on a select number of Impact Washington web pages hosting program information and interest forms. This data allowed for further examination of the time that stakeholders spent on these pages after navigating to them from emails.

**Key Findings:** Unique open and click-through rates over the course of grant demonstration confirm that the network is consistently “reachable,” and it often takes time and consistency to reach them. The email delivery rate is high, indicating integrity in the lists used to contact DoD Contractors.

Once the eblasts were delivered, the likelihood that recipients open the emails was consistently strong and in line with industry benchmarks that range from 18-21%.

Outreach	1										
Outreach Type/Title	Email: Programs and Funds to Simulate Manufacturing Growth										
Audience	Impact Washington Newsletter Subscribers										
Message/Call to Action	Awareness of Commerce’s Investment in Defense and CMMC										
	<table><tr><th>Email Date</th><th># Emails Sent</th><th>Delivery Rate</th><th>Open Rate</th><th>Unique Click-Through Rate</th></tr><tr><td>8.20.2020</td><td>4,927</td><td>100%</td><td>20% (990)</td><td>2.6% (130)</td></tr></table>	Email Date	# Emails Sent	Delivery Rate	Open Rate	Unique Click-Through Rate	8.20.2020	4,927	100%	20% (990)	2.6% (130)
Email Date	# Emails Sent	Delivery Rate	Open Rate	Unique Click-Through Rate							
8.20.2020	4,927	100%	20% (990)	2.6% (130)							
Links to forms, pages, and Blog Posts	<p><b>Blog:</b> <a href="#">Washington State Department of Commerce Invests in Defense Manufacturers with Cybersecurity Training</a> August 17, 2020   Aerospace, Cybersecurity, News Releases</p> <p><b>Blog:</b> <a href="#">DFARS and Understanding the DoD’s Cybersecurity Maturity Model Certification (CMMC) Training Set for Early Fall</a> August 18, 2020   Aerospace, Cybersecurity, News Releases</p>										

Outreach	2										
Outreach Type/Title	Email: Cybersecurity Help for the Washington State Defense Supply Chain companies – Letter from Impact Washington Center Director										
Audience	DoD list from Commerce and PNDC										
Message/Call to Action	Awareness of Commerce’s Investment in Defense and CMMC, Announcement of Fall CMMC Online Training										
	<table><tr><th>Email Date</th><th># Emails Sent</th><th>Delivery Rate</th><th>Open Rate</th><th>Unique Click-Through Rate</th></tr><tr><td>9.8.2020</td><td>3,594</td><td>99%</td><td>13% (473)</td><td>1.6% (59)</td></tr></table>	Email Date	# Emails Sent	Delivery Rate	Open Rate	Unique Click-Through Rate	9.8.2020	3,594	99%	13% (473)	1.6% (59)
Email Date	# Emails Sent	Delivery Rate	Open Rate	Unique Click-Through Rate							
9.8.2020	3,594	99%	13% (473)	1.6% (59)							
Links to forms, pages, and Blog Posts	<p><b>Web Page:</b> <a href="#">Understand Your Cybersecurity</a> Maturity Model (CMMC) Readiness</p>										

Outreach	3										
Outreach Type/Title	Impact Washington – September Newsletter										
Audience	Impact Washington Newsletter Subscribers plus DoD List										
Message/Call to Action	Pre-registration is still open: Impact Washington is offering no-cost DFARS and CMMC training to members of the Washington State defense supply chain.										
	<table><tr><th>Email Date</th><th># Emails Sent</th><th>Delivery Rate</th><th>Open Rate</th><th>Unique Click-Through Rate</th></tr><tr><td>9.28.2020</td><td>8,421</td><td>99%</td><td>14% (1193)</td><td>.9% (73)</td></tr></table>	Email Date	# Emails Sent	Delivery Rate	Open Rate	Unique Click-Through Rate	9.28.2020	8,421	99%	14% (1193)	.9% (73)
Email Date	# Emails Sent	Delivery Rate	Open Rate	Unique Click-Through Rate							
9.28.2020	8,421	99%	14% (1193)	.9% (73)							
Links to forms, pages, and Blog Posts	<p><b>Web Page:</b> <a href="#">Understand Your Cybersecurity</a> Maturity Model (CMMC) Readiness</p>										

Outreach	4										
Outreach Type/Title	Email: Cybersecurity Maturity Model Certification (CMMC) Readiness Courses Update										
Audience	Individuals who pre-registered for CMMC Courses										
Message/Call to Action	<p><b>Update: On availability of Courses (Available Mid-October).</b> Ask recipients to encourage their supply chain members to sign-up for the no-cost courses to ensure all tiers along your supply chain understand the upcoming requirements and register for courses.</p>										
	<table><tr><th>Email Date</th><th># Emails Sent</th><th>Delivery Rate</th><th>Open Rate</th><th>Unique Click-Through Rate</th></tr><tr><td>10.8.2020</td><td>100</td><td>100%</td><td>40% (37)</td><td>.9% (9)</td></tr></table>	Email Date	# Emails Sent	Delivery Rate	Open Rate	Unique Click-Through Rate	10.8.2020	100	100%	40% (37)	.9% (9)
Email Date	# Emails Sent	Delivery Rate	Open Rate	Unique Click-Through Rate							
10.8.2020	100	100%	40% (37)	.9% (9)							
Links to forms, pages, and Blog Posts	<p><b>Web Page:</b> <a href="#">Understand Your Cybersecurity</a> Maturity Model (CMMC) Readiness</p>										

Outreach	5				
Outreach Type/Title	Email: Cybersecurity Maturity Model Certification (CMMC) Readiness Courses:				
Audience	Individuals who pre-registered for CMMC Courses				
Message/Call to Action	<p>Register: CMMC self-pace courses now available.</p> <p>Ask: Recipients to encourage their supply chain members to sign-up for the no-cost courses to ensure all tiers along your supply chain understand the upcoming requirements and register for courses</p>				
Links to forms, pages, and Blog Posts	Email Date	# Emails Sent	Delivery Rate	Open Rate	Unique Click-Through Rate
	10.23.2020	100	100%	40% (4)	0
	Web Page: : <a href="#">Self-Paced, Online Training</a>				

Outreach	6				
Outreach Type/Title	Impact Washington – October Newsletter				
Audience	Impact Washington Newsletter Subscribers + DoD List				
Message/Call to Action	Article: National Cybersecurity Month Announcement of One-On-One Cybersecurity Support for Washington State to Businesses in DoD Supply Chain – Fill out Application				
Links to forms, pages, and Blog Posts	Email Date	# Emails Sent	Delivery Rate	Open Rate	Unique Click-Through Rate
	10.26.2020	8,422	100%	11% (943)	.95% (79)
	Web Page: <a href="#">Understanding DFARS &amp; CMMC</a> Registration Page: <a href="#">Cybersecurity One-On-One Pilot Program</a> Article Link: <a href="#">Cybersecurity Awareness Month: If You Connect It, Protect It.</a>				

Outreach	7				
Outreach Type/Title	Email: Don't Miss Your Opportunity for CMMC Support				
Audience	DoD list from Commerce and PNDC				
Message/Call to Action	Message: Find information on our website or reach out to cyber@impactwashington.org Apply: for One-One-One Support   Register: for No-Cost CMMC Readiness Training				
Links to forms, pages, and Blog Posts	Email Date	# Emails Sent	Delivery Rate	Open Rate	Unique Click-Through Rate
	11.11.2020	3,512	100%	10% (355)	1.9% (67)
	Web Page: <a href="#">Understanding DFARS &amp; CMMC</a> Contact us at <a href="mailto:cyber@impactwashington.org">cyber@impactwashington.org</a> Registration Pages: <a href="#">Cybersecurity One-On-One Pilot Program</a>   <a href="#">Self-Paced, Online Training</a>				

Outreach	8				
Outreach Type/Title	CMMC Readiness Courses - Login Reminder				
Audience	Those who signed-up for CMMC Courses but did not complete				
Message/Call to Action	Message: CMMC Readiness Courses Now Available Don't Miss Your Opportunity to Participate!				
Links to forms, pages, and Blog Posts	Email Date	# Emails Sent	Delivery Rate	Open Rate	Unique Click-Through Rate
	12.7.2020	86	100%	47% (40)	13% (11)
	Registration Page: <a href="#">Self-Paced, Online Training</a>				
	Registration Page: <a href="#">Self-Paced, Online Training Forgot Password</a>				

Outreach	9										
Outreach Type/Title	Impact Washington – January Newsletter										
Audience	Impact Washington Newsletter Subscribers										
Message/Call to Action	<b>Article: Need Help Preparing for CMMC</b> Article: Which Manufactures Are at Risk for Cyber Attacks Event Recap: PIVOT to Defense PNDC Event										
Links to forms, pages, and Blog Posts	<table><tr><th>Email Date</th><th># Emails Sent</th><th>Delivery Rate</th><th>Open Rate</th><th>Unique Click-Through Rate</th></tr><tr><td>1.25.2021</td><td>5,523</td><td>100%</td><td>13% (723)</td><td>3% (168)</td></tr></table>	Email Date	# Emails Sent	Delivery Rate	Open Rate	Unique Click-Through Rate	1.25.2021	5,523	100%	13% (723)	3% (168)
	Email Date	# Emails Sent	Delivery Rate	Open Rate	Unique Click-Through Rate						
	1.25.2021	5,523	100%	13% (723)	3% (168)						
<b>Registration Page:</b> <a href="#">Self-Paced, Online Training</a> <b>Web Page:</b> <a href="#">Impact Washington Cyber Consulting</a> <b>Contact Us:</b> <a href="#">Contact Us with Questions</a>											

Outreach	10										
Outreach Type/Title	Impact Washington – February Newsletter										
Audience	Impact Washington Newsletter Subscribers										
Message/Call to Action	Article: Need Help Understanding Cybersecurity or Preparing for CMMC? Register: Self-Paced, E-Learning For DFARS/NIST 800-171 courses still available Defense Supply Chain.										
Links to forms, pages, and Blog Posts	<table><tr><th>Email Date</th><th># Emails Sent</th><th>Delivery Rate</th><th>Open Rate</th><th>Unique Click-Through Rate</th></tr><tr><td>2.26.2021</td><td>5,509</td><td>100%</td><td>12% (684)</td><td>.87% (48)</td></tr></table>	Email Date	# Emails Sent	Delivery Rate	Open Rate	Unique Click-Through Rate	2.26.2021	5,509	100%	12% (684)	.87% (48)
	Email Date	# Emails Sent	Delivery Rate	Open Rate	Unique Click-Through Rate						
	2.26.2021	5,509	100%	12% (684)	.87% (48)						
<b>Registration Page:</b> <a href="#">Self-Paced, Online Training</a>											

Outreach	11										
Outreach Type/Title	Impact Washington – March Newsletter										
Audience	Impact Washington Newsletter Subscribers										
Message/Call to Action	Article: Assessing Your Company’s Cybersecurity Risks and Implementing Controls to Protect Your Business’s Data Does Not Have to Be Overwhelming. Invitation: Complete this our One-On-One Pilot Program Registration Form. Register: Self-Paced, E-Learning For DFARS/NIST 800-171 courses still available										
Links to forms, pages, and Blog Posts	<table><tr><th>Email Date</th><th># Emails Sent</th><th>Delivery Rate</th><th>Open Rate</th><th>Unique Click-Through Rate</th></tr><tr><td>3.18.2021</td><td>6,016</td><td>100%</td><td>20% (1221)</td><td>4.1% (247)</td></tr></table>	Email Date	# Emails Sent	Delivery Rate	Open Rate	Unique Click-Through Rate	3.18.2021	6,016	100%	20% (1221)	4.1% (247)
	Email Date	# Emails Sent	Delivery Rate	Open Rate	Unique Click-Through Rate						
	3.18.2021	6,016	100%	20% (1221)	4.1% (247)						
<b>Registration Page:</b> <a href="#">Cybersecurity One-On-One Pilot Program</a> <b>Registration Page:</b> <a href="#">Self-Paced, Online Training</a>											

Outreach	12										
Outreach Type/Title	Impact Washington – April Newsletter										
Audience	Impact Washington Newsletter Subscribers										
Message/Call to Action	Register: Self-Paced, E-Learning For DFARS/NIST 800-171 courses still available Event Invitation: Microsoft Partner CMMC Journey Webinar Event Invitation: to Impact Washington and PNDC Lessons Learned Webinars										
Links to forms, pages, and Blog Posts	<table><tr><th>Email Date</th><th># Emails Sent</th><th>Delivery Rate</th><th>Open Rate</th><th>Unique Click-Through Rate</th></tr><tr><td>4.13.2021</td><td>6,005</td><td>100%</td><td>16% (975)</td><td>3.4% (204)</td></tr></table>	Email Date	# Emails Sent	Delivery Rate	Open Rate	Unique Click-Through Rate	4.13.2021	6,005	100%	16% (975)	3.4% (204)
	Email Date	# Emails Sent	Delivery Rate	Open Rate	Unique Click-Through Rate						
	4.13.2021	6,005	100%	16% (975)	3.4% (204)						
<b>Registration Page:</b> <a href="#">Self-Paced, Online Training</a> <a href="#">May 5th - Complying with DoD Cybersecurity Requirements – What Have We Learned?   Informational Webinar</a> <a href="#">May 18th Complying With DOD Cybersecurity Requirements – Where to Start   Informational Webinar</a> <a href="#">June 3rd Lessons Learned In Supporting Constituent’s Cybersecurity Journey   Informational Webinar</a>											

## Webinar Outreach

Following is a summary of the webinars conducted during the course of the grant period. To constructively view the effectiveness of the webinars, we reviewed the following metrics:

- ✓ Overall Attendee Ratio: Out of all the people who registered for your webinar, how many attended the live broadcast? This information can tell you how interesting the audience finds your webinar topics.
- ✓ DoD Contractor Attendee Ratio: Out of all the people who registered for your webinar, how many of those who attended the live broadcast are part of the DoD?

Post-webinar ‘thank you’ emails were sent to all participants to show appreciation and further our relationship with the audience. Post-emails included a post-webinar survey asking for opinions on presentations and topics for future webinars.

All webinars were recorded for re-purposed content. Videos were added to YouTube channels and embedded into web pages and relevant blogs.

## Webinar Topics, Dates and Metric Report

**Title** Understanding And Complying with The Department of Defense's (DoD) New Cybersecurity Maturity Model Certification (CMMC) Seminar\*

**Goal** Awareness of CMMC Requirements

Webinar Date	# Registered	Attendee Ratio	WA State DoD Supply Chain Ratio	Unique WA Companies
3.31.2020	39	72% (28)	415 (16)	14

**Average Attendee Evaluation Score** 4.7 out of 5 | **Link** [https://www.youtube.com/watch?v=EeMB\\_JayBNY](https://www.youtube.com/watch?v=EeMB_JayBNY)

**Title** Understanding And Complying with The Department of Defense's (DoD) New Cybersecurity Maturity Model Certification (CMMC) Seminar\*

**Goal** Awareness of CMMC Requirements

Webinar Date	# Registered	Attendee Ratio	WA State DoD Supply Chain Ratio	Unique WA Companies
4.9.2020	118	79% (93)	71% (84)	58

**Average Attendee Evaluation Score** 4.5 out of 5 | **Link** <https://www.youtube.com/watch?v=98h1oEwbeKY>

**Title** Cybersecurity Resiliency for Defense Contractors

**Goal** Update on CMMC Requirements and launch of LMS

Webinar Date	# Registered	Attendee Ratio	WA State DoD Supply Chain Ratio	Unique WA Companies
8.6.2020	348	58% (205)	41% (142)	119

**Average Attendee Evaluation Score** 4.5 out of 5 | **Link** <https://www.youtube.com/watch?v=S5osLLd2SnY>

**Title** Complying With DoD Cybersecurity Requirements – What Have We Learned

**Goal** Update and lessons learned through grant program – target CMMC Level 3 businesses

Webinar Date	# Registered	Attendee Ratio	WA State DoD Supply Chain Ratio	Unique WA Companies
5.5.2021	111	66% (73)	45% (50)	41

**Average Attendee Evaluation Score** 4.4 out of 5 | **Link** <https://youtu.be/d6hQGA4mY48>

**Title** Complying With DoD Cybersecurity Requirements – Where to Start

**Goal** Update and lessons learned through grant program – target CMMC Level 1 & 2 businesses

Webinar Date	# Registered	Attendee Ratio	WA State DoD Supply Chain Ratio	Unique WA Companies
5.18.2021	94	57% (54)	49% (46)	40

**Average Attendee Evaluation Score** 4.5 out of 5 | **Link** <https://studio.youtube.com/video/wuhM3PuPBpY/edit>

**Title** Lessons Learned in Supporting Constituent's Cybersecurity Journey

**Goal** Update and lessons learned through grant program – for organizations looking to support their constituents CMMC compliance.

Webinar Date	# Registered	Attendee Ratio	WA State DoD Supply Chain Ratio	Unique WA Companies
6.3.2021	42	66% (28)	NA	NA

**Average Attendee Evaluation Score** 4.3 out of 5 | **Link** <https://www.youtube.com/watch?v=991Zjqr5-M>

\* Originally planned as in-person events, one serving Puget Sound and one serving SW Washington, were held online due to COVID.

## LMS Training Participation

Two CMMC Compliance Training courses were created and offered on the LMS platform to better understand and prepare for DoD's CMMC.

Courses were no cost to members of the Washington defense supply chain. We extended invitations to ecosystem partners to participate in the courses at no cost. Organizations outside the state were allowed to participate and charged a nominal fee.

**1. The Senior Management Course focuses on the importance of cybersecurity in protecting company assets and resources and outlining the measures and resources needed to achieve compliance.**

**2. The Practitioner Course facilitates and identifies the steps needed to move the company toward DFARS and CMMC compliance.**

Individuals could complete both courses.

### SENIOR MANAGEMENT COURSE DETAILS

#### About This Course:

This course provides a general overview of the DFARS standards and NIST 800-171 and how they relate to emerging CMMC compliance requirements. Participants will go through the origins of CMMC, its essential core components, and what the DoD will expect. This path will also illustrate that in addition to technical requirements, much of CMMC compliance is non-technical and involves the implementation of cybersecurity best practices. The course will enable you to think critically about the importance of cybersecurity, recognize its place in your company's risk management strategy, and visualize a path to achieve compliance.

#### Who Should Attend:

CEOs, Procurement Specialists, and senior managers with legal, financial, and compliance responsibilities.

#### What you will learn:

- ✓ Compare the DFARS standards, NIST 800-171, and the CMMC domain requirements.
- ✓ Interpret barriers and challenges of cybersecurity compliance.
- ✓ Communicate the steps and resources required in the CMMC readiness process.
- ✓ Connect sources of support to achieve DFARS and CMMC compliance.
- ✓ Determine a path for DFARS and CMMC audit readiness.

Length: 20 minutes (self-paced)

Training Completion Document: Upon course completion.

### PRACTITIONER COURSE DETAILS

#### About this course:

This course will unpack the alignment of the DFARS standards and NIST 800-171 with the 5 levels of CMMC, focusing on level 3. Modules will illustrate the process for implementing all the required standards and practices for DoD compliance and provide guidance, resources, and tools for preparing and submitting a CMMC certification package.

**Who Should Attend:**

Operations managers, HR professionals, Engineering/IT, and other technical personnel.

Length: 40-60 minutes (Self-paced instruction + additional time for the Toolbox)

Training Completion Document: Upon course completion.

**What you will learn:**

- ✓ Assess your current and future contracts to DFARS standards, NIST 800-171, and emerging CMMC requirements.
- ✓ Evaluate your current cybersecurity processes and practices against DFARS, NIST 800-171, and the emerging CMMC level requirements.
- ✓ Establish and implement a gap analysis between your current processes and practices and DFARS, NIST 800-171, and CMMC standards.
- ✓ Review, draft, and revise your system security plan to meet DFARS standards and NIST 800-171, and establish a pathway to CMMC compliance.

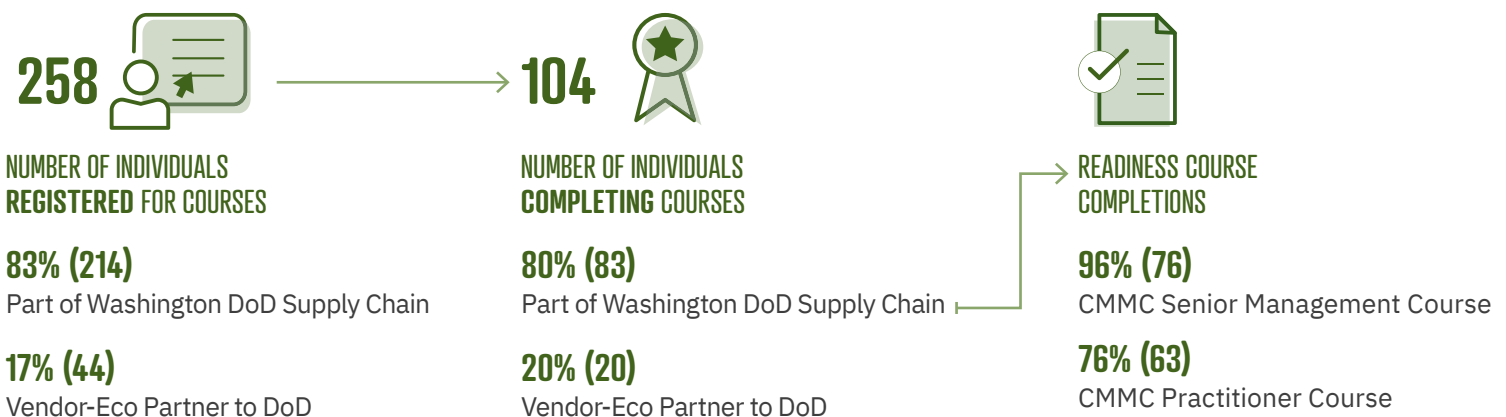
**Toolbox:** CMMC Training Modules provide participants with the tools and resources to self-manage and progress toward their organization's compliance. Participants will learn CMMC material through interactive sessions while joining a larger pool of candidates. These tools will enable participants to create roadmaps, track milestones, and control the entire process to manage cybersecurity and move toward compliance.

**Online Training Outcomes:**

Impact Washington began promoting and accepting preregistration for the online CMMC Compliance Training in early September 2020. In total, 258 individuals representing 81 companies signed up to take one or both courses.

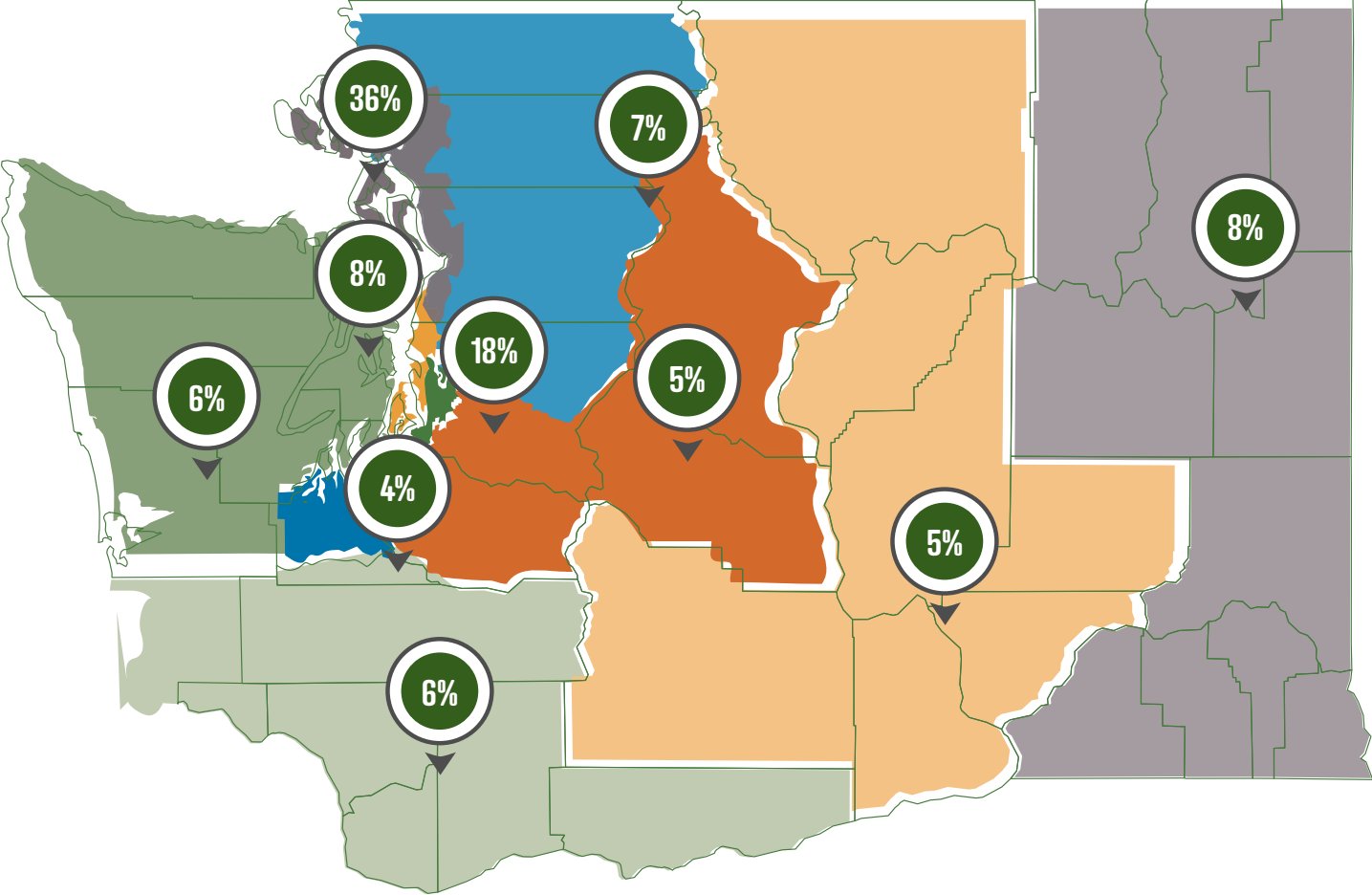
Four out of ten (40%) who preregistered completed one or both courses. Most of those individuals (80%) are from a business in the defense supply chain or interested in supplying defense agencies (directly or in the supply chain).

Many individuals took advantage of the opportunity to take both courses. The majority (65%) of individuals completed all modules on the same day they registered. Others registered and then revisited the lessons and modules using their unique sign-in and password to complete the course(s). Emails sent on October 8th, October 23rd, and December 7th reminded individuals to complete the courses.



With the help of our outreach partners we were able to facilitate statewide participation in course.

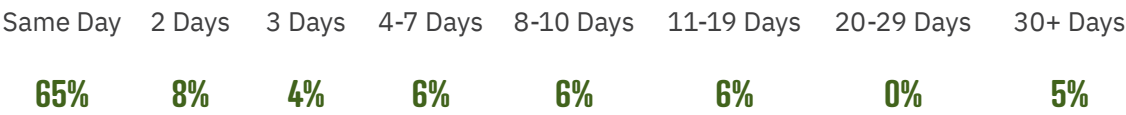
% Individuals within DoD Supply Chain Participating by Congressional District (Sample Size = 83)



- |                  |                  |
|------------------|------------------|
| District 1   7%  | District 6   6%  |
| District 2   36% | District 7   5%  |
| District 3   6%  | District 8   5%  |
| District 4   5%  | District 9   18% |
| District 5   8%  | District 10   4% |

Most individuals were able to finish the course(s) in a timely manner.

% Number of Days for Individuals to Complete the Course(s)  
(Sample Size = 83 Individuals within DoD Supply Chain)



## BUDGET REVIEW

Cost of activities undertaken within the grant were \$974,805 against a budget of \$975,000; \$195 under budget.

ELEMENTS	BUDGET	ACTUAL	SURPLUS/ (DEFICIT )	SURPLUS/ (DEFICIT) %
<b>CYBER RESILIENCY</b>				
Indirect Costs	50,000	47,200		
Compliance Platform Development & Licensing		148,200		
Client Assessment & Expert Support		323,400		
<b>Cyber Resiliency Subtotal</b>	<b>500,000</b>	<b>518,800</b>	<b>(18,800)</b>	<b>(3.8%)</b>
<b>CYBER INDEPENDENCE</b>				
Indirect Costs	47,500	41,455		
Project Management		90,750		
Outreach		40,100		
Training Development		114,400		
Training Delivery		142,000		
Grant Impact Webinars and Reporting		27,300		
<b>Cyber Independence Subtotal</b>	<b>475,000</b>	<b>456,005</b>	<b>18,995</b>	<b>4.0%</b>
<b>TOTAL PROJECT</b>	<b>975,000</b>	<b>974,805</b>	<b>195 (0.0%)</b>	

Because the outreach and training elements of the grant were revised due to prevailing circumstances, the Cyber Independence element of the grant was under spent by nearly \$19,000 (4.0%). This enabled additional funding to be allocated to the Cyber Resiliency element resulting in support of 36 members of the defense supply rather than the 19 outlined in the grant design.

As allowed in Attachment B of the Services Contract, “The total amount of transfers between line item budget categories [Cyber Resiliency and Cyber Independence] shall not exceed ten (10) percent of the grant.”

## NEXT STEPS

This grant funded by the Department of Defense Office of Local Defense Community Cooperation (DoD OLDCC) through the Washington State Department of Commerce Office of Economic Development and Competitiveness enabled the initiation of a strong public/private ecosystem supporting members of the Washington State defense supply chain to strengthen their cybersecurity posture and advance their Cybersecurity Maturity Model Certification (CMMC) readiness. Through the period of performance of the grant, awareness of the need for cybersecurity compliance steadily increased due to the outreach efforts of Impact Washington and its partners. Additionally, awareness significantly amplified with the November 30, 2020, DoD DFARS interim rule that effectively confirmed the DoD Assessment Methodology and CMMC framework implementation. The release of this interim rule confirmed for many in the DoD supply chain that active pursuit of improved cybersecurity posture was a good idea and a requirement for participation in the DoD supply chain.

In addition to engaging many in the public support ecosystem such as chambers of commerce, economic development councils, advocacy organizations, etc., the project team was surprised and pleased with companies' strong engagement in the private sector, the cybersecurity service providers (CSPs). Of course, there is a commercial motivation from the CSPs to connect with new clients. Still, there was also a strong sense of mission in assisting the DoD supply chain members in improving their cybersecurity posture.

Constituents of the DoD supply chain are significant in number. Within this cohort of CSPs, there was a collaborative atmosphere to share ideas and methodologies to develop cybersecurity services more expediently and cost-effectively. Perhaps because the number is so great, there was a feeling that developing better means of delivering services would benefit all.

Although there has been a positive shift in awareness, there are still significant impediments to SMBs undertaking a program to advance their cybersecurity posture, as outlined earlier in this report. Perhaps the most prevalent constraint is cost or fear of unknown

expenses. In almost every instance of clients served in guided support, grant funding was vital to securing a decision for clients to engage. The grant project team believe that grants or other forms of financial aid will continue to be critical to engage the DoD supply chain members.

Advancing cybersecurity posture is considered a mission-critical imperative in the NIST MEP network. Specifically with Impact Washington, short-term grant support for other Washington State manufacturers will continue beyond the end of the period of performance of this grant utilizing various other funding sources.

Work continues with the strong network of public and private partners to build on the momentum enabled and created by this grant funding. Application for longer-term cybersecurity grant funding is being sought. Additional funding will allow Impact Washington to continue providing the cybersecurity support members of the Washington DoD supply chain and all manufacturers require to maintain and advance their status as world-class competitors.

In response to a 2021 NIST Notice of Funding Opportunity, Impact Washington submitted a nearly \$2M proposal to continue and extend its support of cybersecurity education and implementation for manufacturers in the state of Washington. The proposal aims to expand no-cost access to competency-based educational offerings specific to CMMC implementation. It also provides significant grant support for no less than 100 small to medium-sized manufacturers (SMMs) to implement NIST 800-171 and CMMC requirements over three years, extending to 2024. The proposal, if successful, will build upon crucial relationships with other Pacific NW NIST MEP Centers and ecosystem partners such as DoD, aerospace, maritime, and food industry trade associations. Regardless of funding mechanisms, the goal is to build a sustainable cybersecurity support community for SMMs in Washington state and the Pacific NW that will allow them to be competitive and productive partners in the DoD and broader industrial supply chains.

## ACKNOWLEDGMENTS

Impact Washington is greatly appreciative of the Department of Defense Office of Local Defense Community Cooperation (DoD OLDCC) for providing this grant funding to support members of the Washington State defense supply chain in advancing their cybersecurity posture.

The Washington State Department of Commerce Office of Economic Development and Competitiveness continues to be a key partner in advancing companies' success and competitive position within the state. Impact Washington is honored to have been selected to deliver critical elements of the grant project.

Execution of the grant activities could not have been done without the support and collaboration of Impact Washington's talented and dedicated group of partners, notably the Pacific Northwest Defense Coalition (PNDC) and the Washington Procurement Technical Assistance Center (Washington PTAC).

Finally, Impact Washington acknowledges the collaboration of all our competent and committed private sector partners. They worked assiduously to elevate the cybersecurity posture of their assigned members of the Washington State defense supply chain. There was great experience gained and learning done that will enable us to support others in the future.



## APPENDIX A

### CSP's Scope of Work

#### Introduction

Impact Washington is requesting proposals from qualified contractors to assist in conducting programmatic elements of initial cybersecurity & DFARs assessment and consulting for members of the Defense supply chain in Washington State to fulfill a related grant's requirements.

#### Key Dates

Deadline for submission of RFP responses: Friday, September 25, 2020

Work completion date: Monday, May 31, 2021

#### Table of Contents

- Introduction
- Key Dates
- Background
- Scope of Work
- Expected Work-products & Deliverables
- Work location & execution
- Pricing & Level of Effort
- Questions
- Rejection of Bid Proposals
- Disqualification
- Reference Checks
- Information from Other Sources
- NDA Signature Required
- Contractor Conflict of Interest
- Proposal Submission Instructions
- Evaluation Criteria

#### Background

Impact Washington (IW) is a non-profit organization that provides competitive, value-driven services to enhance growth, improve productivity, reduce costs, and expand manufacturing capacity in Washington State. We are an affiliate of the National Institute of Standards and Technology's Manufacturing Extension Program (NIST MEP), and our solutions, consulting, and educational opportunities focus on the small & medium-sized manufacturers located throughout the state.

IW has been awarded a cybersecurity grant by the Department of Defense (DoD) Office of Economic Adjustment through the Washington State Department of Commerce, with the broad intent of strengthening Washington State Defense's cyber-security posture supply chain. Work performed under the grant will focus on two core elements – Cyber Independence and Cyber Resiliency.

The intent of Cyber Independence is to provide outreach to all known Defense suppliers in Washington to create awareness of DoD cybersecurity requirements and provide more in- depth training with at least 10% of that population.

Cyber Resiliency will focus on conducting broad and tactical asset-value based cyber assessments for 1% of the known Defense suppliers (19 companies), evaluating results, and providing recommendations for correction.

Further work under the grant will provide one-on-one support engagements with the 1% of the companies that have participated in the cyber resiliency element to move their negative resiliency responses to cybersecurity compliance.

## Scope of Work

Nineteen (19) private companies will receive one-on-one support, as outlined in the introduction above. It is intended that the work will be divided between 3 – 5 contractors to build regional capacity and expertise in engaging the private market to benefit those companies involved in these initial engagements and establishing options to support the broader Defense supply chain in the future.

Accordingly, each selected Contractor will receive contracts to work with 4 – 7 companies. IW has contracted a third party, Ignyte Institute (Ignyte), to provide self-paced, e-learning, and an assurance management platform for reporting and tracking client progress - the Ignyte Certification and Accreditation Platform (Platform).

The Platform manages compliance, vendor risk, business continuity, threat management, and learning management through a single interface for Small to Medium-sized Businesses (SMBs). Platform technology fully integrates with current standard SMB operational security toolsets such as Qualys, Tenable, KnowBe4, and other operational toolsets to ensure compliance. Included within the connector eco-system is full integration with DoD level tools such as SAM and Enterprise Mission Assurance Support Service (eMASS). This technology for the SMB will help accelerate compliance & cybersecurity processes end to end. The Platform is expected to be used by the bidder's analyst to complete SMB cyber tasks. Team members from Ignyte will provide training & on-boarding.

## Impact Washington (IW) Engagement Methodology

**Contractors must follow IW prescribed methodology in managing and leading the engagement.**

- ✓ At the start of the engagement, IW will provide proper scoping information.
- ✓ The Contractor must identify themselves to IW as potential future “CMMC Auditor” and/or “Registered Consultant.”
- ✓ IW is to lead as the primary Contractor and provide back-end support for managing contractual obligations with the selected private company.
- ✓ IW will provide all contract documentation to support cyber activities for the target SMB.
- ✓ Leverage the use of the Platform. Platform training and usage will be provided directly to the assigned security analyst.
- ✓ A single license of the Platform will be assigned to the organization.
- ✓ Project reporting, performance tracking, and work-products deliverables are to be captured within the Platform.
- ✓ Report & debrief IW assigned project manager on tasks & work completed.
- ✓ Complete a brief project plan per organization provided by IW team before engagement starts.

## Initial Cybersecurity & DFARs Assessment Scope of Work

**Each engagement must quickly capture and assess the following within each private organization leveraging the Platform:**

- ✓ Organization chart
- ✓ Organization departments

- ✓ Organization locations
- ✓ Current IT and/or security policies (if any)
- ✓ Current known Security Classification Guides as provided by DoD (if any)
- ✓ A complete Asset Inventory, including the following elements:
  - Hardware (Servers, network devices, end-user devices)
  - Critical Business Software
    - SaaS Services, ERP systems, etc...
- ✓ The following critical asset inventory attributes must be identified:
  - CUI and CUI Type (a list of CUI and CUI type will be provided)
  - Sensitive business information according to a standardized classification scheme within the Platform
  - Relate all assets with organizational departments & locations
  - Determine the qualitative impact of business systems
    - Determine the cyber impact of business systems based on C, I, A values
- ✓ Capture other attributes such as RTOs & RPOs per asset as optional attributes
- ✓ Capture additional optional asset attributes such as known vulnerabilities, EOL, etc... (optional attributes for assets containing aggregated CUI). Please see the intrusive technology section on determining vulnerabilities.
- ✓ A complete asset record is desired; however, assets that contain CUI shall be the focus of the assessment.
- ✓ Policy & Documentation records per organization:
  - Place all documents collected within a structured folder system within the Platform
    - Policies, Procedures, Guidelines, Evidence, CUI Contract Documents
- ✓ Promote the training provided by Impact Washington to reduce the cost of training for the assigned SMB.
- ✓ Capture training records from the Ignite LMS and place it within the compliance area, specifically the “Awareness & Training” domain of CMMC and/or NIST 800-171.
- ✓ Conduct an Initial Draft CMMC framework assessment based on level 3. An initial evaluation must include the following:
  - Review of each requirement by the assigned security analyst.
  - Provide an expert opinion summary response per requirement based on discussion with the private company.
  - Capture each requirement’s current status according to the CMMC draft framework (Performed, Documented, Managed, Reviewed, Optimized).
  - Attachments of any documentation provided by the organization to each NIST 800-171 requirement. Documentation should be uploaded to structured folders as well as provided within the Platform.
- ✓ Any NIST 800-171 requirement with the current status of “Performed” a POA&M will be automatically generated.
- ✓ A recommendation on how to “document” the requirement shall be provided within the POA&M summary section. A recommendation must include the following:
  - Recommended policy & procedure name for gap closure and a brief description of the policy and/or missing procedure.

- Optional automation technologies can be recommended within the control/practice statement and/or within the POA&M. However, if an organization is missing critical documentation, it must be identified within the automatically generated POA&M.
- ✓ Company SSP and POA&M will be automatically generated by the Platform based on structured work completed for the SMB.
- ✓ A client level, analyst level, and multi-level per company dashboard will be automatically generated based on the work completed.
- ✓ The estimated level of effort per requirement range shall be provided to IW for determining the competitiveness of your offer and understanding of your draft CMMC requirements.

## Usage of Impact Washington Resources Provided

One of this grant's fundamental goals is to help SMBs by leveraging resources provided under the grant. The Contractor shall leverage these resources as part of the engagement as cost reduction efforts include the following. Over time, IW will release additional resources to benefit the IW community:

- ✓ CMMC self-paced, e-learning courses
- ✓ CMMC pre-assessment tool kit (if required)
- ✓ Ignite pre-certification Platform to create a system of record
- ✓ Provided project plan (if required)
- ✓ Provided scoping worksheet
- ✓ Policies and procedures templates (as developed over time)
- ✓ Outline or IW Team members (account manager, project managers & collaborative cyber partners)

## Intrusive Technology Usage limitations and Basic Rules of Engagement

IW has determined that the highest need is to help SMBs prepare for winning future defense contracts while helping retain current agreements is to ensure robust DoD contract activity and a healthy local State of Washington economy.

This goal is achieved by assisting SMBs to prepare for executive risk management & cyber assurance activities primarily and technical security operational tasks as secondary items.

IW also has determined that it does not desire to engage in high-profile attacks, threat modeling, defense and offensive security exercises, web-application attacks, and external inspection scoring systems targeted at small businesses.

This preparation includes leveraging a basic rating system to inspect the small business website, SSL certificates checks, external corporate traffic, etc.... that may not contain any sensitive information, including CUI. It also includes conducting & interpreting vulnerability tests that could lead to the exploitation of a small business network. The essence and intent of this sort of activity is captured within the asset-value based portion of the Initial Cybersecurity & DFARS Assessment Scope of Work.

Determination of location CUI, aggregation of CUI, assets cyber impact, business impact, and asset value to the organization will set the potential scope of technical surveillance, continuous monitoring, penetration testing, vulnerability testing, threat modeling, and similar operational security work in the near future. Engagement should be focused on management level cyber risk & assurance management coaching to increase local manufacturing leaders' technical literacy before engaging in highly specialized activities that lead to minimal value without management support.

## Expected Work-Products and Deliverables

### To be delivered & organized within the Platform

- ✓ Summary response per DFARs and/or Draft CMMC Requirement (estimated 130 requirements for Level 3)
- ✓ POA&M responses & corrective recommendations within POA&M (where applicable)
- ✓ Critical Asset inventory with up to 20 crucial attributes per asset
- ✓ Current documentation (policies, procedures, screenshots, evidence of meeting requirements) from the organization.
- ✓ Reference of relevant documents to each requirement

## Work Location and Execution

IW recognizes the impact of COVID-19 and envisions that this entire engagement could be delivered remotely, with assessments conducted via teleconference calls. However, agreement with IW, Contractor, and on-site client work can be done assuming State-mandated safety measures are in place and observed.

## Pricing and Level of Effort

IW goal is to build a regional capacity of expertise for both current and future partner work through Impact Washington to help grow the state's defense industrial base. Your proposal should reflect pricing based on the level of effort and required analyst skillset. The price should be provided as a range per company based on the target market that IW traditionally serves and scope described within the Initial Cybersecurity & DFARs Assessment Scope of Work paragraph.

## IW Target Market

### IW serves constituents with the following characteristics:

- ✓ Typical organization size of 10 – 200 employees
- ✓ Typically led by a non-technical business leader with a strong manufacturing background
- ✓ Small IT staff (1-3 people) and /or completely outsourced IT staff
- ✓ 1 to 50 Critical Assets that may contain CUI and/or sensitive business information

## Questions

We invite bidders to submit written questions and requests for clarifications regarding the RFP. IW assumes no responsibility for verbal representations made by its officers or employees unless such representations are confirmed in writing and incorporated into the RFP. Any ambiguity regarding this RFP must be addressed through this question and answer process. Bidders are not permitted to include assumptions in their bid proposals. Please direct all your questions to IW via email at Geoff Lawrence glawrence@impactwashington.org

## Rejection of Bid Proposals

IW reserves the right to reject any or all bid proposals, in whole and part, and cancel this RFP at any time prior to executing a written contract. Issuance of this RFP in no way constitutes a commitment by the IW to award a contract.

## Disqualification

IW reserves the right to reject outright and not evaluate proposals for any one of the following reasons:

- ✓ The bidder states that a service requirement cannot be met.
- ✓ The bidder fails to deliver the bid proposal by the due date and time.
- ✓ The bidder fails to deliver the detailed cost section.
- ✓ The bidder's response materially changes a service requirement.
- ✓ The bidder's response limits the rights of the IW
- ✓ The bidder initiates unauthorized contact regarding the RFP with IW partners and employees.
- ✓ The bidder provides misleading or inaccurate responses.

## Reference Checks

IW reserves the right to contact any reference to assist in evaluating the bid proposal, verify the information contained in the bid proposal, and discuss the bidder's qualifications and the qualifications of any subcontractor identified in the bid proposal.

## Information from Other Sources

IW reserves the right to obtain and consider information from other sources concerning a bidder, such as a bidder's capability and performance under different contracts.

## NDA Signature Required

Bidder must sign an NDA with IW, private companies, and IW partners to protect IW resources, company sensitive information, and partner resources provided to contractors to fulfill this grant's requirements.

## Contractor Conflict of Interest

The bidder shall submit any Conflict of Interest information to IW regarding IW ability to partner with other cybersecurity teams. For this contract's purposes, the conflict of interest definition includes direct or indirect relationships, including, but not limited to, the Contractor and its parent company, subsidiaries, affiliates, subcontractors, clients, and principals.

## Proposal Submission Instructions and Due Date

The bidder's proposals must be sent via email by close of business Friday, September 25, 2020 to:  
**Impact Washington, Geoff Lawrence, [glawrence@impactwashington.org](mailto:glawrence@impactwashington.org)**

**The bidder's proposal must include the following areas:**

1. Title page
2. Overview of your our work experience in cybersecurity and your organization's experience
  - Expected goal to become a consulting organization and audit organization (C3PAO)
3. Scope of work with all the sub-sections addressed.
4. Expected Deliverables
5. Estimated timelines & cost per company assessment

## Evaluation Criteria

The Impact Washington Panel Review will evaluate each proposal individually against the following criteria, listed below in order of importance, and not against competing bids. Please use the below criteria as a reference but do not structure your proposal according to the sub-sections.

### 1. Cost-effectiveness & best value for small businesses.

IW strongly encourages bidders to demonstrate project cost-effectiveness in their approach, including examples of leveraging IW institutional and other resources. However, cost-sharing or other examples of leveraging other resources are not needed. The inclusion of cost-sharing in the budget does not result in additional points awarded during the review process. Budgets should have low and reasonable overhead and administration costs, and applicants should provide clear explanations and justifications for these costs concerning the work involved. All budget assessment items need to be explained and justified to demonstrate necessity, appropriateness, and connection to the project objectives.

### 2. Technical approach

IW encourages bidders to demonstrate their technical approach per the Scope of Work Expected Work- products & Deliverables. A substantial bidder will include a clear articulation of how the assigned analyst will complete the desired activities to contribute to the overall IW cybersecurity project objectives as part of a single seamless team working with up to 5 small businesses.



## APPENDIX B

### List of Cybersecurity Service Provider (CSP's) Partners Participating in Grant

---

#### CORTAC GROUP

**jerry.leishman@cortacgroup.com | (877) 216-1717 | [www.cortacgroup.com](http://www.cortacgroup.com)**

CORTAC Group is a national professional services company that brings Defense, Aerospace and Commercial suppliers a holistic approach to systems and information protection and governance, regulatory compliance, and competitive strategies to Keep and Win More Business. Its client base includes many top-tier defense contractors and supporting supply chain sub-contractors in the Pacific Northwest as well as commercial companies. It has an office in Seattle area to serve NW clients.

**Services Offered:** Regulatory & cybersecurity assessments and due care, business and technical solution planning and implementation, audit preparation, regulatory compliance operations, business capture, analytics, and program management.

**Size/Type of Businesses Served:** All sizes.

---

#### TOTEM TECHNOLOGIES

**info@totem.tech | (855) 405-4075 | [www.totem.tech](http://www.totem.tech)**

Totem has over a decade of experience securing and monitoring US Government and DOD IT systems, including classified and controlled unclassified information (CUI). Totem does a lot of cybersecurity work for the federal government, but their passion is helping other contractors with Cybersecurity Maturity Model Certification (CMMC) and NIST 800-171 compliance.

**Services Offered:** Cybersecurity Consultants for Defense Contractors.

**Type of Businesses Served:** Small to Medium sized businesses in the Defense Industrial Base.

---

#### INTECH

**raj@intechnw.com | (206) 397-8070 | [www.inTechNW.com](http://www.inTechNW.com)**

inTech provides Information Technology services including Compliance and Risk Management to manufacturing companies in the Pacific Northwest. They are based in Kent, Washington with offices throughout the area.

**Services Offered:** inTech provides Managed Information Technology services including Compliance and Risk Management to manufacturing companies in the Pacific Northwest. They are based in Kent, Washington with offices throughout the area. They have helped many companies manage their challenges related to their technology and compliance needs. Other services provided are: Technology Consultation, Penetration Testing, Internal & External Vulnerability Scanning and Remediation, Managed end-user training, Managed monthly phishing campaigns.

**Type of Businesses Served:** Small and Medium sized business.

---

## FUTURE NETWORKING (FNI, INC.)

**talktous@futurenetworking.com | (503) 684-9002 | [www.futurenetworking.com](http://www.futurenetworking.com)**

FNI mitigates risk so your business can thrive. Our in-depth compliance approach provides your company a strong foundation for securing and maintaining defense contracts. Robust cybersecurity is FNI's mission. Our solutions help protect your intellectual property and support national security. Because our staff has CMMC Registered Practitioner, Security+, and related certificates, you can be confident we deliver DFARS, ITAR and CMMC compliance expertise. FNI's pending application for C3PAO status demonstrates you have a partner dedicated to compliance now and into the future.

**Services Offered:** CMMC, DFARS, ITAR compliance assistance. Compliant backup and recovery. MSP and Compliance as a Service (CaaS). Cloud services.

**Type of Businesses Served:** Small to medium DIB companies.

---

## HOW TO GRC LLC

**learn@howtogrc.com | (907) 299-7775 | [www.howtogrc.com](http://www.howtogrc.com)**

HowToGRC is a full service advisory and audit firm focused on providing end-to-end practical SCF based solutions to DoD suppliers and their subcontractors.

**Services Offered:** CMMC Advisory and Audit, ISO27001 Advisory and Audit, NIST 800-171/DFARS Compliance, Cybersecurity Education and Training, Supply Chain Risk Management.

**Type of Businesses Served:** Manufacturing, Services, Construction, Aerospace, Software, Telecommunications.

---

## LUMINANT DIGITAL SECURITY

**info@luminantsecurity.com | (503) 905-3285 | [www.luminantsecurity.com](http://www.luminantsecurity.com)**

CMMC-AB approved RPO & RP with a C3PAO application pending approval. It takes expert guidance and a culture of security to defend your business from ever-changing threats. When you seek to deploy a robust CMMC cybersecurity program, Luminant's partnership prepares you for whatever situations arise. Through their Secure Care and Compliance Care monthly managed cybersecurity service plans, they will help your company implement and manage a formal cybersecurity program based on CMMC and be your consultative guide as new requirements and demands on your business come up.

**Services Offered:** CMMC Managed Cybersecurity Services, CMMC Readiness Assessments, Penetration Testing, User Training, Phishing, Vulnerability Scans.

**Type of Businesses Served:** Small-to-Midsize Businesses with 20-1000 users in Manufacturing, Construction, Legal & Professional Services.

---

## EDGE NETWORKS

**mark.tishenko@edgenetworks.us | (360) 450-0033 | [www.edgenetworks.us](http://www.edgenetworks.us)**

Edge Networks help you run your Cybersecurity department so you and your team can focus on what you do best. With Edge Networks, you have the peace of mind to focus on the rest of your business.

**Services Offered:** Managed IT and Managed Cybersecurity Services (Compliance, Engineering and Management)

**Size/Type of Business Served:** Small to Medium Size Businesses in the Manufacturing and Professional Service Industries.

---

## EXBABYLON IT SOLUTIONS

**info@exbabylon.com | (509) 447-0440 | [www.exbabylon.com](http://www.exbabylon.com)**

Exbabylon is a full-service Managed IT, Microsoft Cloud and Security Solution Provider based in the Inland Northwest. With a decade of experience serving the Aerospace and Defense industries our team provides vertically aligned, industry specific, cyber compliance with a stack that streamlines IT operations and compliance in one solution built for fully or co-managed environments.

**Services Offered:** Managed IT, Security and CSP

**Size/Type of Business Served:** Small to Medium Businesses (10-500 employees) in fully managed (no internal IT) to co-managed (supporting internal IT teams)

---

## IGNYTE ASSURANCE PLATFORM

**info@ignyteplatform.com | 1.833.IGNYTE1 | [www.ignyteplatform.com](http://www.ignyteplatform.com)**

Ignyte team offers full automation capabilities for all aspects of CMMC Services Offered.

**Services Offered:** Cybersecurity consulting / service and Risk, Compliance management software.

**Size/Type of Business Served:** Small to medium size businesses in manufacturing, finance, healthcare, and other markets.

## APPENDIX C

### Grant Awardees Company Profiles

Company	Congressional District	City	County	Employee Size-Self Reported	Industry	SBA Self-Designation
Advanced Technology Construction	10	Tacoma	Pierce	40	Construction	
Applied Technical Systems (ATS)	6	Silverdale	Kitsap	23	Architectural, Engineering, & Related Services	Service-Disabled Veteran-Owned Small Business
AR Modular RF	1	Bothell	King	38	DIB	Hubzone
Carbon Consultants LLC, dba Zepher	3	White Salmon	Klickitat	52	Aerospace	EDWOSB
Chi-Chack LLC	6	Tacoma	Pierce	145	Government Contracts	Vet Owned
ControlTek, Inc.	3	Vancouver	Clark	115	Electronics	
Darbonnier Tactical Supply DTS LLC	2	Oak Harbor	Island	27	DoD Gov't. Sales	
Data Enterprises of the Northwest, Inc.	9	Bellevue	King	5	Software Publishing	
Delphi Precision Imaging Corporation	1	Redmond	King	6	Aerospace	
Electroimpact	2	Mukilteo	Snohomish	600	Aerospace Tooling	
Evergreen Fire Alarms, LLC dba Evergreen Fire and Security	10	Tacoma	Pierce	80	DoD System Integrator	
General Plastics Manufacturing Co.	6	Tacoma	Pierce	150	Manufacturing	
GM Nameplate	7	Seattle	King	900	Manufacturing	
Hobart Machined Products Inc.	8	Hobart	King	5	Manufacturing	Woman owned
Holmes Mechanical, Inc.	6	Bremerton	Kitsap	29	Plumbing & Mechanical	
Huntron Inc	1	Mill Creek	Snohomish	10	Contractor	
Hyssos Tech LLC	10	Olympia	Thurston	2	Defense	
Jemco Components and Fabrication	1	Kirkland	King	110	Aerospace	Woman owned
Kinetics, Inc.	3	Stevenson	Skamania	4	SW R&D	
King Machine, LLC	2	Mukilteo	Snohomish	47	Machine Shop	
Lighthouse for the Blind	9	Seattle	King	473	Social Services	
LKD Aerospace LLC	8	Snoqualmie	King	29	Aerospace	
Makers Architecture	7	Seattle	King	31	Architecture & Engineering	Woman owned
Mantel Technologies	10	Steilacoom	Pierce	11	Scientific Research & Development Services	
Perellion	2	Lynnwood	Snohomish	4	Aerospace	
PNDC - Pacific Northwest Defense Coalition		Las Oswego	Oregon		Professional Services	
Proctor Products Co, Inc.	2	Arlington	Snohomish	19	Aerospace Tooling	
Silicon Forest Electronics Inc.	3	Vancouver	Clark	82	Electronics Mfg.	
Stack Metallurgical Group	5	Spokane	Spokane	110	Metal Processing	
Technical Tooling	9	Tacoma	Pierce	6	Aerospace & Defense	
TMF, Inc.	6	Poulsbo	Kitsap	12	Defense	
TNT AEROSPACE	1	Sumas	Whatcom	5	Aerospace	
US Aluminum Castings	8	Entiat	Chelan	60	Foundry	
Vet Industrial	6	Bremerton	Kitsap	19	Construction	
Veterans Northwest Construction	7	Seattle	King	18	Construction	
Xplore, Inc.	9	Mercer Island	King	10	Space	

## APPENDIX D

### Totem Curriculum

# TOTEM'S VIRTUAL CLASSROOM

1

#### OVERVIEW OF REQUIREMENTS

Overview of DFARS/CMMC/NIST 800-171 cybersecurity compliance requirement

2

#### SCOPING YOUR PLAN

System Inventory basics - Introduction to the System Description workbook

3

#### INITIAL ASSESSMENT

The DoD's official Assessment Methodology - how the DoD will score your cybersecurity program

4

#### BUILDING AN SSP (PART 1)

Learn the System Security Plan (SSP) requirements and provide an introduction to Cybersecurity Program Planning

5

#### BUILDING AN SSP (PART 2)

Principles of quality cybersecurity policies and prioritizing implementation by addressing the FAR17

6

#### BUILDING AN SSP (PART 3)

Addressing other challenging control families

7

#### INCIDENT RESPONSE PLANNING (PART 1)

Learning how to report incidents, obtain an ECA certificate, and understanding Incident Response Plan basics

8

#### INCIDENT RESPONSE PLANNING (PART 2)

Exercising your Incident Response Plan

9

#### CLOSING THE GAPS

Developing and executing a Plan of Actions and Milestones (POA&M) and answer and lingering questions

**CLASSES RUN FOR 3 WEEKS**

## LEARNING OBJECTIVES

- Understand the requirements for a DoD contractor cybersecurity program
- Understand how the DoD intends to assess and certify cybersecurity programs for compliance
- Begin building a System Security Plan (SSP) as a set of “blueprints” for their organization’s cybersecurity program
- Begin developing a compliant and efficient cyber Incident Response capability within their organization
- Understand how to develop and execute corrective action plans to fix gaps between current state of cybersecurity plan implementation and that outlined in the SSP

## APPENDIX E

### Detailed Engagement Client Reports

DoD Supply Chain Client	What is your overall satisfaction with the Cybersecurity Service Provider?	What is your overall satisfaction with the software provided as part of this engagement? (provided by Ignyte or Totem Technology)?
1	Very Satisfied	Satisfied
2	Satisfied	Satisfied
3	Satisfied	Neutral
4	Very Satisfied	Satisfied
5	Very Satisfied	Very Satisfied
6	Very Satisfied	Very Satisfied
7	Satisfied	Satisfied
8	Very Satisfied	Neutral
9		
10	Satisfied	Satisfied
11	Neutral	Disatisfied
12	Disatisfied	Neutral
13	Neutral	Neutral
14	Satisfied	Neutral
15	Very Satisfied	Satisfied
16	Satisfied	Satisfied
17	Very Satisfied	Satisfied
18	Very Satisfied	Very Satisfied
19	Satisfied	Neutral
20	Very Satisfied	Very Satisfied
21	Very Satisfied	Very Satisfied
22	Very Satisfied	Very Satisfied
23	Very Satisfied	Satisfied
24	Satisfied	Neutral
25	Very Satisfied	Satisfied
26	Very Satisfied	Neutral
27	Very Satisfied	Very Satisfied
28	Very Satisfied	
29	Satisfied	Neutral
30	Satisfied	Neutral
31	Neutral	Neutral
32	Very Satisfied	Satisfied
33	Neutral	Neutral
34	Very Satisfied	Very Satisfied
35	Very Satisfied	Very Satisfied
36	Satisfied	Satisfied

## ROADBLOCKS TO STARTING THE ENGAGEMENT

DoD Supply Chain Client	Fear of unknown costs	Lack of focused staff time	No internal project manager	Lack of awareness that all DoD contractors must comply	Lack of perceived ROI	No impeding/clear deadline from DoD
1		✓				
2	✓	✓				
3	✓					✓
4						✓
5	✓	✓				✓
6		✓				✓
7	✓	✓				✓
8	✓				✓	✓
9						✓
10						✓
11			✓		✓	✓
12	✓	✓			✓	✓
13						✓
14					✓	
15	✓	✓	✓	✓	✓	✓
16	✓	✓				✓
17						✓
18	✓					✓
19				✓	✓	
20	✓					
21	✓	✓	✓			
22		✓				
23	✓	✓		✓	✓	
24		✓				
25	✓					
26		✓				
27	✓					
28	✓	✓				
29	✓	✓	✓			
30	✓	✓				
31	✓	✓	✓			
32	✓	✓				✓
33	✓					
34	✓		✓			
35	✓					✓
36						✓

## TOTAL STAFF TIME DEVOTED TO CYBERSECURITY IN 2021, INTERNAL OR OUTSOURCED

DoD Supply Chain Client	Management / Executive (hours)	IT Staff Time (hours)	Administrative Staff Time (hours)
1	50	100	
2	8	40	8
3	240	200	
4	100	1040	
5	100	500	250
6	60	20	10
7	100	50	2
8	100	700	
9			
10			
11	200	2000	
12	34	2804	60
13	60	120	10
14	40	120	
15	100	30	
16	20	20	40
17	48	24	0
18	80	400	
19	UNKNOWN	UNKNOWN	UNKNOWN
20	80	120	20
21	40		240
22	500	1000	0
23	40	500	
24	30	5	5
25	20	40	20
26	300		
27	200	500	0
28	5		30
29	120	120	
30	60	500	150
31	60	0	20
32	400	400	400 - one day per week for first year est
33	34	6	N/A
34	90	20	5
35	60	20	
36	100	500	0

## PLANS FOR MANAGING ONGOING CYBERSECURITY COMPLIANCE (CHECK ALL THAT APPLY)

DoD Supply Chain Client	Full time IT Staff	Part Time IT Staff	Full Time Cybersecurity Staff	Part Time Cybersecurity Staff	Managed IT Service Provider (outsourced)	Managed Cybersecurity Service Provider (outsourced)	Other - Write In (Required)
1	✓			✓			
2	✓			✓			
3		✓			✓		
4		✓					
5					✓	✓	
6	✓					✓	IT contactor (as needed for specific tasks))
7		✓			✓		
8		✓			✓		
9							
10					✓		
11	✓						
12	✓						On retainer- outside cybersecurity consultant
13		✓				✓	
14	✓						
15							Unknown
16					✓	✓	
17					✓	✓	
18		✓					
19					✓		
20					✓		
21							Part-time designated from current staff
22	✓				✓	✓	
23					✓		
24		✓		✓		✓	
25	✓				✓	✓	
26							We are small, our management team will continue to carry the load on this requirement it's the only fiscally reasonable solution.
27				✓	✓		
28					✓	✓	
29					✓		
30	✓				✓	✓	
31							Not yet determined
32					✓		existing staff with rearranged priorities
33					✓	✓	
34				✓	✓		Management shared responsibility
35					✓		internal management lead, with outsourced IT Provider
36	✓						

**In addition to your company's funds to participate in this Pilot Program, did you have any additional expenses, such as hardware, software, software as a service (SaaS), subscriptions, etc. in 2021**

DoD Supply Chain Client	Description 1	Cost 1	Reoccurrence of Cost 1 *
1	Server Upgrade	\$70,000	
2			
3			
4	Solarwinds	\$16,000	one-time (2020)
5	MSP	\$1000.00+	Monthly
6	Servers	\$6,500	One-time
7	yes, but unknown yet		
8	Not yet		
9			
10			
11	KnowBe4 Security Awareness Training	\$4,000	Annually
12	All listed	\$61,000 - \$65,000	Annually
13	Managed security service provider fees (Monitoring, SIEM, vulnerability scanning)	\$3,000	Monthly
14			
15	Work with managed service provider	\$15,000	
16			
17	Not Determined yet		
18	Not yet		
19	Unknown		
20	Software	\$15,000	Annually
21	hardware and software	\$2,000	one-time
22	MSSP	\$50,000	Annually
23	SIEM/SOC	\$60,000	Annually
24	Cybersecurity Service Provider	\$25,000	0
25			
26	We already have Google Workspace, Jumpcloud and PCMATIC costs		
27	On premise server and firewall	\$19,000	
28	Upgrade to Drop Box	\$100	Monthly
29			
30			
31	None		
32	Application upgrades	Unknown Still	one-time
33	System Scan	247.5	one-time
34	None		
35	Coordination Meeting with outsourced IT	\$2,500	one-time
36	software, firewalls, consulting	\$50,000	will be more next year

\*(Monthly, Annually, One-time, etc.)

**In addition to your company's funds to participate in this Pilot Program, did you have any additional expenses, such as hardware, software, software as a service (SaaS), subscriptions, etc. in 2021**

DoD Supply Chain Client	Description 2	Cost 2	Reoccurrence of Cost 2 *
1	Upgraded all estimating and project software	\$20,000	
2			
3			
4	Solarwinds (5 products)	\$5,800	Annually
5	Office365 GCC	\$1000.00+	Monthly
6	Laptops	\$10,000	One-time
7	yes, but unknown yet		
8	Currently evaluating software options		
9			
10			
11	Compliance Forge Compliance NIST Compliance Program Documentation Package	\$4,480	One-time
12	See above		Annually
13			
14			
15			
16			
17	Not Determined yet		
18			
19	Unknown		
20	Hardware	\$20,000	N/A
21	Software and Services	\$800	Annually
22	MSP	\$40,000	Annually
23	MFA	\$5,000	Annually
24	Enclave Provider	\$15,000	\$23,000 /Annually
25			
26			
27			
28	MS 365 Upgrades (MFA, etc.)	\$50	Monthly
29			
30			
31	None		
32	Application updates	Unknown Still	ongoing, prop annually
33	N/A		
34	None		
35			
36			

\*(Monthly, Annually, One-time, etc.)

In addition to your company's funds to participate in this Pilot Program, did you have any additional expenses, such as hardware, software, software as a service (SaaS), subscriptions, etc. in 2021

DoD Supply Chain Client	Description 3	Cost 3	Reoccurrence of Cost 3*
1			
2			
3			
4			
5			
6	Monitors	\$5,000	One-time
7	yes, but unknown yet		
8	Currently evaluating software options		
9			
10			
11			
12	All Listed		Annually
13			
14			
15			
16			
17	Not Determined yet		
18			
19	Uknown		
20			
21			
22	Hardware/Software	\$30,000	One-time
23	Hardware/Encryption	\$15,000	Annually
24			
25			
26			
27			
28			
29			
30			
31	None		
32			
33	N/A		
34	None		
35			
36			

\*(Monthly, Annually, One-time, etc.)

**In addition to your company's funds to participate in this Pilot Program, did you have any additional expenses, such as hardware, software, software as a service (SaaS), subscriptions, etc. in 2021**

		Most recent Supplier Performance Risk System (SPRS) cybersecurity score (if known)	
DoD Supply Chain Client	Any Other Costs?	Before Engagement	After Engagement
1	No	Unknown	Unknown
2			
3		21	
4	In 2018, we spent \$80k on hardware upgrades to support CMMC3. In 2019, we spent \$20k to update switches.	None	Will file for CMMC3
5		-210	-97
6		-89	N/A
7	yes, but unknown yet	-208	-98
8	Substantial Time - which we expect to continue to work on in 2021 as well as some limited software and service expenditures.	54	56
9			
10			
11		-156	-156
12	Additional costs may be added to accommodate growth- such as server racks, virtual servers, upgrades to data privacy tools, etc.	min requirement	TBD
13	We are anticipating the CSP will be recommending additional services such as Office 365 GCCH. These will be evaluated once we have the final report out from the CSP.	43	108
14	N/A	N/A	N/A
15		16	30
16		50	53
17	Not Determined yet	Unknown	38
18	Not yet as we don't have a contract forcing us to comply....	-254	-144
19	No costs at this current time have not started working on implementing NCRs to correct issues yet		
20	No	84	Unknown
21	There will certainly be increased costs in the near future as we work through complying with the controls we are not meeting yet.		
22		-3	56
23	Antivirus with AI - Annual cost ~\$12,000	78	84
24	Not at this time	-35	57
25			
26	We may need to add an encryption layer. Still evaluating		
27	Lots more to come over the next year.	-68	50
28			
29			

**In addition to your company's funds to participate in this Pilot Program, did you have any additional expenses, such as hardware, software, software as a service (SaaS), subscriptions, etc. in 2021**

		Most Recent Supplier Performance Risk System (SPRS) Cybersecurity Score (if known)	
DoD Supply Chain Client	Any Other Costs?	Before Engagement	After Engagement
30	Not yet, we haven't finished the new POAM.	38	38
31	We are currently assessing how we will meet the level 3 through outsourcing. Researching cost and the comparative value each vendor would bring.	N/A	N/A
32	We will mostly likely know these details in August. We've had many services in place through our MSP prior to starting.		
33	Projected cost of new ERP system....roughly \$6500 up front	Unknown	Unknown
34	None		
35	There will be many future costs, entry control, cameras, possibly Managed Security Service Provider as well as numerous software and hardware purchases	-181	-81
36	We expect our costs to increase as our company grows.		

## Cybersecurity Progress

DoD Supply Chain Client	Did you have a cybersecurity incident this year (ransomware, phishing attack, etc)?	Did you tout your cybersecurity maturity in a bid or sales conversation this year?	Did you improve a business process through implementing the cybersecurity program?
1	YES	NO	NO
2	NO	YES	YES
3	NO	NO	YES
4	NO	NO	YES
5	NO	NO	YES
6	NO	NO	NO
7	NO	NO	YES
8	NO	NO	YES
9			
10	NO	NO	UNKNOWN
11	YES	NO	NO
12	NO	UNKNOWN	YES
13	NO	YES	NO
14	NO	NO	YES
15	NO	YES	YES
16	NO	NO	NO
17	NO	NO	UNKNOWN
18	YES	YES	YES
19	NO	NO	UNKNOWN
20	NO	YES	NO
21	NO	NO	YES
22	NO	NO	NO
23	YES	NO	YES
24	NO	YES	YES
25	NO	NO	NO
26	NO	NO	NO
27	NO	YES	YES
28	YES	NO	YES
29	NO	NO	NO
30	NO	NO	NO
31	YES	NO	UNKNOWN
32	NO	NO	YES
33	NO	YES	NO/UNKNOWN
34	NO	NO	YES
35	NO	NO	YES
36	NO	NO	YES



**When asked what the most valuable aspect of the engagement with the Cybersecurity Service Provider was, participants responded:**

- It helping me to keep my data safe and allowing me to work with Federal Department of Defense clients.
- CSP had good knowledge of the CMMC framework and is willing and available for any questions or input.
- Provided a good balance and overview of the CMMC program and the key elements of to focus on.
- They provided a full assessment of the 130 controls. Reviewed of our work and provided expertise to identify gaps.
- Very clear and engaging lectures. Depth of knowledge and clear guidance on compliance was very appreciated.
- Evaluating our business practices and determining appropriate scope for CMMC
- Working with a Provider that completely knew the program's requirements, and is committed to remaining up-to-date as they may change.
- Effective interaction with consultant with good response time. Valuable feedback on the interpretation/scope for some of the controls, Independent review of our internal assessment and guidance on needed solutions.
- We were provided with a sample architecture, some timeline information, and some pricing information which we can use as guidelines for our planning.
- Knowing what artifacts would be required for an auditor.
- Having an assessment done by certified auditors. This helps us understand not only what needs to be done to improve our security posture but what an auditor would be looking for. This should prepare us for our CMMC later this year.
- Building a plan for CMMC compliance, help with understanding CMMC controls, eye opening to current issues and problems.
- They know the requirements and understand how to move towards achieving compliance.
- Not having to do it ourselves
- CSP was knowledgeable and engaging.
- Explained the CMMC process and provided continuing access to a cyber resource.
- Seeing all of our areas needing to be improving, and knowing where we stand when it comes to security.
- Coaching and patience
- The most valuable aspects of the engagement was to have the Cybersecurity Service Provider as someone to 1) guide us on evaluating our current posture related to CMMC compliance, 2) be accountable to through the process, and 3) set a framework for making progress and moving forward.
- The small business perspective and the fact that it is a lot of work but using the tools provided you just keep moving forward.
- Our provider was able to connect us with an enclave provider who is a better solution for us.
- CSP was very knowledgeable, responsive and clearly communicated expectations. I couldn't have asked for a better consultant
- Expert guidance and a sounding board to help us focus in areas where we were overlooking deficiencies.
- The most valuable aspect for us was that the service provider is a small business like we are, so they take the approach of how to meet the CMMC requirements without the substantial resources of a large company.
- Knowledge of the CMMC requirements and how we can comply using as much of our current technology and processes as possible.
- Learned a ton about what the specific requirements are related to the pending CMMC implementation.
- Having an outside set of eyes explain to management the importance of compliance.
- Having the ability to ask questions as we were working through the Domains and requirements to meet a level 3 certification.
- The one on one discussions. CSP's assistance with interpretation of the requirements has been extremely helpful. He also understands the challenges that small businesses face.
- Organization
- Explaining process and providing templates and framework.
- Important for us to learn about this topic from a knowledgeable source, and CSP met that criteria.



**When asked what would you suggest to improve your work with the Cybersecurity Service Provider, participants responded:**

- We are grateful for the support and need more funding for programs such as this one.
- CMMC development updates and resources should be made more readily available to the end user so that the provider is not the sole source of the most current information.
- The course was very condensed --recommend to extend by a week to absorb all the material
- It would have been better if they could have provided policy templates that we could edit. They did not even have a concept of the policies that would be required for certification.
- We would have actually appreciated the training time to go more in-depth on each topic but understand time is limited all around.
- More regular check-ins about status and progress
- Ideally we would have understood the policy shortcuts (mirroring CMMC control structure) recommendations early to save time. We also thought that there were some procedure templates that were available that we could request/leverage that would help us forward our documentation quicker.
- It was hard to coordinate time with the provider, partly due to a lack of ownership interest in security work dragging out the contract state date, and partly because the provider seemed overextended and had to bring on outside resources to provide deliverables. I felt like we were presented with some general information due to a shortness of one-on-one time to describe the unique aspects of our systems.
- Better communication and responsiveness to include transparency on expectations.
- More expertise on government regulations- auditor had no experience on CMMC or expectations of government systems on the commercial level.
- He used a checklist and did not do a deeper dive into findings or look into actual documentation. (We could have done the checklist ourselves without them.)
- So far the experience has been excellent.
- In person meetings or site visit to increase productivity

- Always could use more time and details but overall the tool provided has much needed information.
- Our provider offers top notch cybersecurity solutions however they had very little experience with enclave solutions which is what we ultimately selected.
- Happy with the service it was very flexible and tailored to our needs.
- More hands on with going through actual writing of compliance documents within the training.
- Consolidated list of providers or programs that may address requirements (bonus if they are other small businesses). For example IDS/IPS intrusion detection system/intrusion Prevention Systems Options: Security Onion, Snort, Zeek & Suricata or Security Information and Event Management (SIEM): Security Onion(free), Perch, Alien Vault(totem uses), Splunk Loggly (solar winds)



**Progress made on the cybersecurity journey through this engagement;**

- This helped with our strategic plan for implementation
- Internal assessment/audit underway.
- Got the POAM developed and having a clear scope on the IT boundary for complying with CMMC
- Contractor reviewed 130 CMMC3 controls; Contractor Review of 10 existing policies; We created 11 new policies Contractor provided their assessment on the Ignyte platform; Contractor trained us on Ignyte platform
- We established a SSP and PoaM and established a base-line for where we are at with compliance.
- Our Provider (ignyte) led us through the first several steps, providing documentation frameworks and technical expertise so that we were able to: -better understand the scope of requirements -complete and submit our SPRS -complete our IS Security Policy document -assist us with identifying vendors
- Transition from 800-171 to CMMC SSP/POAM. Good substantiation of current posture, some control and documentation improvement. Requirements clarification/ plan on many key controls.

- We didn't really make any progress, other than to reinforce our gaps
- We have practices in place that address all 110 controls.
- We are at the very beginning. We now have information to take positive steps toward compliance and a resource to turn to for help.
- Submitted self assessment score to SPRS. Drafted company policies for cyber security awareness, training, access control, and security program. Identified & logged all IT assets.
- Just getting started
- Understand process better.
- A baseline of where we stand
- Major progress
- We made great progress in gaining an understanding of our cyber security baseline, and what understanding what is missing and where we need to get to. This engagement gave us the start we needed in order to understand where we need to go. We learned a lot from the Cyber Service Provider, who helped us set a plan and evaluate our current posture. The next steps will be to fine-tune our current policies, and then to begin evaluating options and implementing the controls we are missing.
- Compliant with NIST 800-171 requirements
- Enclave provider has created a secure cloud based storage and sharing solution and is reviewing our self assessment to create an SSP and POAM.
- We are CMMC level 1 compliant and well on our way to CMMC level 2
- Working towards a better set of documentation on compliance steps/procedures/policies/processes.
- We have made a ton of progress, but this is only just beginning. We have one year of consulting with CSP to advance our posture.
- Developed plan to meet CMMC level 1 requirements.
- This was a learning experience for me. We did figure out that an enclave was the best approach, so we're able to get started on the SSP.
- We received a current state report against CMMC Level 3, an SSP "CAN" be exported based on this information ,and a POAM "CAN" be created. I believe the project is wrapped though so it will be on us to generate. Possibly with consultant help.
- We have a working knowledge of the domains required to meet a level 3 cert. We identified GAPS and have a completed GAP assessment.
- Documentation. Working with the cybersecurity consultant has lifted our mental blocks to getting them started.
- CMMC plan and compliance
- I have a much better understanding of the process, and have multiple plans started, and completed the SSP. I have in addition to the start of the POAM a list of things that can be accomplished quickly.
- We now have an SSP and PO&AM in a much more advanced state, and a more structured approach to making progress on actions to be implemented.



**When asked if there were any roadblocks stopping progress in your cybersecurity compliance journey, participants responded:**

- Time and money are the largest barriers
- Dedicated staffing time.
- Beside costs, and time we lack in-house expertise and have had to look to outside consultants.
- Lack of sufficient internal IT resources to execute changes
- Lack of focused staff time availability (common to all small businesses)
- We will continue progressing - staff time and costs will be some factors impeding progress.
- Ownership is having to make hard choices with money and cut overhead due to the aviation downturn. It's hard to convince them to spend money and time on CMMC when it won't be required for years to come.
- 1. Cost 2. Skills gap- Cybersecurity specialist 3. Database development and infrastructure professional
- Report out from CSP, costs of additional tools/services for compliance. We are targeting CMMC level 3 but it is unknown when this is truly required by our customers. Our customers also seem unsure of when we would need certification. Not knowing this makes it challenging when trying to budget.
- Legacy systems and the need for them.

- No, just dedicating the time required to finish the process.
- funding and time.
- Just more money... which is always hard to find
- Moving forward, time and lack of a dedicated staff position will be a roadblock moving forward. There may be some financial roadblocks in the future as we weigh our options for meeting some of the controls. No longer having someone we are accountable to guiding us through the process may also set us back. However, the Cyber Service Provider has worked with us on a plan to continue to make progress internally. The other roadblock we may run into moving forward is no longer having a go-to expert in cyber security.
- Cost of the MSSP provider and how to justify for the amount of Defense work we do. There is no way a small company can do all the auditing so it has to be outsourced and cost is big.
- Man hours and cost
- Time/money
- The reoccurring cost of adding things like an MSSP and SIEM tool are challenging for our small business.
- Budget. Staff Hours. Consultant Hours (Budget but also availability). Working against our MSP when they don't perform, having to backtrack to fix things. Executive engagement. The fact that Ignyte did not have CMMC controls to score against. It still does not have MFA. Clunky to use. Cost is high.
- We are a small company, hours to devote to the process is challenging as we do not have an IT or security position to rely upon.
- Time and Resources. If we have to go to a Managed Security Service Provider, then we have not budgeted for this cost. With a small company without the resources or internal IT it causes a strain to get continued progress.
- Resources continue to be limited for specialized in-house support.
- While we have been impressed with the knowledge the CSP has regarding CMMC and cybersecurity, we are excited to work with them because they understand that solutions need to be tailored around our business practices rather than the other way around. There is still much work to be done for us to reach full compliance with CMMC Level 3 but we are confident that we have chosen the right partner to guide us on this journey.
- As a company leader with minimal experience in cybersecurity, we would not be well on our way to CMMC understanding and compliance had Impact Washington not provided assistance. We would have been at high risk of losing our government business, which would have had a catastrophic effect on our company. Thank you, Impact Washington!
- Our prior SPRS score had several unknowns/gaps. The post score was better afterward and had bolstered several areas where we had marginal support.
- We're still in the early phases of developing our cybersecurity program and have not progressed far enough to see many benefits. We're having a hard time defining scope and have a lot of specific or difficult questions that weren't able to be answered. We appreciate the work performed by the provider but we don't feel that the money spent brought great value.
- The Ignyte tool doesn't seem quite ready and I hesitate putting too much effort in managing our data in the tool. I would have preferred to have a choice of tools or to use the dollars earmarked for the Ignyte subscription for more consulting time or some other service.
- We look forward to getting to a point where we feel confident using our cybersecurity maturity to market ourselves in proposals. This process has helped set us up to better make the progression needed to get there!
- We are thankful the grant allowed us to continue the journey towards level 3 certification. Thank you! Moving forward we will need to devote even more time for Cybersecurity Vendor research/implementation and document preparation all of which will have to be budgeted.
- Just like to get this completed sometime....
- This program has a good intent, but puts a significant strain on resources and I know that many subcontractors will not achieve this in a timely manner unless they simplify things.
- We have benefitted from this grant in that it provided structure and guidance we were considering sourcing independently.



### Other notes or comments:

- CMMC3 is definitely a provides a high level of security for the company. However, it is very expensive to implement and maintain.

## APPENDIX F

### Detailed CSP Reports

DoD Supply Chain Client	Number of company assets/end points	Company's SPRS score at the beginning of the engagement (if known).	Companies SPRS Score at the end of engagement	Company's System Security Plan (SSP) status	Company's Plan of Action and Milestone (POAM) Status
1	30-70	80	unknown	Drafted	Drafted
2	30-70	86	90	Drafted	Started
3	150-250	82		Drafted	Drafted
4	30-70	21	50	Drafted	Started
5	70-150	-210	-100	Drafted	Started
6	Over 250		40	Drafted	Drafted
7	30-Oct	-129	-19	Drafted	Started
8	30-70	unknown	-98	Drafted	Drafted
9	30-Oct	54	56	Drafted	Drafted
10	150-250		-156	Started	Started
11	150-250			Completed	Completed
12	150-250		56	Started	Started
13	Over 250		-107	Started	Started
14	Under 10			Drafted	Completed
15	70-150		50	Drafted	Drafted
16	70-150		38	Drafted	Drafted
17		-254	-144	Drafted	Started
18	30-70		83	Drafted	Drafted
19	Under 10			Drafted	Completed
20	30-70	56	Unknown	Drafted	Drafted
21	Over 250	72	86	Drafted	Drafted
22	Under 10			Started	Drafted
23	30-70			Completed	Drafted
24	Under 10	N/A	N/A	Drafted	Drafted
25	30-70	-68	50	Drafted	Started
26	30-70	43	Unknown	Drafted	Drafted
27	70-150			Started	Started
28	30-Oct			Drafted	Drafted
29	30-70	N/A	62	Completed	Completed
30	30-Oct	N/A	24	Completed	Drafted
31	Under 10		12	Completed	Completed
32	70-150		71	Drafted	Drafted
33	30-70		53	Drafted	Drafted
34	30-70	-181	Unknown	Drafted	Started
35	30-70	-84	Unknown	Drafted	Drafted
36	70-150			Completed	Completed

## Detailed CSP Reports

### CYBER SECURITY READINESS

DoD Supply Chain Client	Company appreciated the need for cybersecurity compliance.		Company had a realistic concept of resources and time required.
1	AGREE	DISAGREE	DISAGREE
2	AGREE	AGREE	AGREE
3	STRONGLY AGREE	AGREE	NEUTRAL
4	AGREE	AGREE	AGREE
5	AGREE	AGREE	AGREE
6	STRONGLY AGREE	STRONGLY AGREE	STRONGLY AGREE
7	AGREE	AGREE	AGREE
8	STRONGLY AGREE	STRONGLY AGREE	AGREE
9	STRONGLY AGREE	STRONGLY AGREE	AGREE
10	STRONGLY DISAGREE	STRONGLY DISAGREE	STRONGLY DISAGREE
11	STRONGLY AGREE	STRONGLY AGREE	STRONGLY AGREE
12	STRONGLY AGREE	NEUTRAL	NEUTRAL
13	STRONGLY AGREE	NEUTRAL	NEUTRAL
14	STRONGLY AGREE	STRONGLY AGREE	AGREE
15	AGREE	AGREE	AGREE
16	AGREE	NEUTRAL	NEUTRAL
17	AGREE	AGREE	AGREE
18	AGREE	NEUTRAL	AGREE
19	AGREE	AGREE	NEUTRAL
20	STRONGLY AGREE	STRONGLY AGREE	STRONGLY AGREE
21	STRONGLY AGREE	AGREE	AGREE
22	STRONGLY AGREE	AGREE	AGREE
23	STRONGLY AGREE	DISAGREE	NEUTRAL
24	STRONGLY AGREE	STRONGLY AGREE	STRONGLY AGREE
25	AGREE	AGREE	AGREE
26	STRONGLY AGREE	STRONGLY AGREE	STRONGLY AGREE
27	AGREE	AGREE	NEUTRAL
28	DISAGREE	STRONGLY DISAGREE	STRONGLY DISAGREE
29	AGREE	DISAGREE	NEUTRAL
30	STRONGLY AGREE	NEUTRAL	DISAGREE
31	AGREE	DISAGREE	AGREE
32	NEUTRAL	NEUTRAL	NEUTRAL
33	NEUTRAL	NEUTRAL	NEUTRAL
34	STRONGLY AGREE	STRONGLY AGREE	STRONGLY AGREE
35	STRONGLY AGREE	STRONGLY AGREE	
36	STRONGLY AGREE	STRONGLY AGREE	STRONGLY AGREE

## Detailed CSP Reports

### COMPANY ROADBLOCKS TO STARTING ENGAGEMENT

DoD Supply Chain Client	Fear of Unknown Costs	Lack of Focused Staff Time	No internal project manager	Lack of awareness that all DoD contractors must comply	Lack of perceived ROI	No impeding/clear deadline from DoD
1	✓	✓				
2	✓					
3		✓	✓			
4	✓					
5	✓					
6						✓
7	✓					
8	✓					✓
9						
10	✓	✓		✓	✓	✓
11						✓
12	✓	✓				
13		✓	✓			✓
14	✓	✓	✓	✓	✓	✓
15	✓		✓			✓
16	✓					✓
17	✓					
18		✓	✓			
19	✓	✓	✓			✓
20	✓					
21				✓		
22	✓					✓
23						✓
24	✓					
25	✓					
26	✓					
27	✓	✓				✓
28	✓	✓	✓	✓	✓	✓
29	✓	✓	✓			✓
30	✓	✓				✓
31	✓	✓			✓	✓
32		✓				
33						✓
34	✓					
35	✓					
36	✓	✓				

## Detailed CSP Reports

### SERVICE PROVIDER OPINIONS CONCERNING FUTURE CYBERSECURITY ACTIVITIES

DoD Supply Chain Client	Company's top management/ ownership was engaged in the process.	Necessary funding and resources were available for the process.	Company will continue to work toward audit readiness.	Company to continue engagement with your organization as a cybersecurity service provider.	Company appreciates the need to continue cyber hygiene and cybersecurity compliance in the future.	Company will budget for continuing cybersecurity activities in the future
1	STRONGLY AGREE	STRONGLY AGREE	STRONGLY AGREE	LIKELY	STRONGLY AGREE	STRONGLY AGREE
2	AGREE	AGREE	AGREE	LIKELY	AGREE	AGREE
3	AGREE	AGREE	STRONGLY AGREE	SOMEWHAT LIKELY	AGREE	STRONGLY AGREE
4	AGREE	AGREE	AGREE	LIKELY	AGREE	AGREE
5	AGREE	AGREE	AGREE	LIKELY	AGREE	AGREE
6	STRONGLY AGREE	STRONGLY AGREE	STRONGLY AGREE	LIKELY	STRONGLY AGREE	STRONGLY AGREE
7	AGREE	AGREE	AGREE	LIKELY	AGREE	AGREE
8	STRONGLY AGREE	NEUTRAL	STRONGLY AGREE	SOMEWHAT LIKELY	STRONGLY AGREE	NEUTRAL
9	AGREE	AGREE	STRONGLY AGREE	LIKELY	STRONGLY AGREE	STRONGLY AGREE
10	DISAGREE	NEUTRAL	DISAGREE	LIKELY	DISAGREE	NEUTRAL
11	STRONGLY AGREE	STRONGLY AGREE	STRONGLY AGREE	SOMEWHAT LIKELY	STRONGLY AGREE	STRONGLY AGREE
12	NEUTRAL	AGREE	NEUTRAL	SOMEWHAT LIKELY	STRONGLY AGREE	STRONGLY AGREE
13	STRONGLY AGREE	STRONGLY AGREE	STRONGLY AGREE	LIKELY	STRONGLY AGREE	STRONGLY AGREE
14	STRONGLY AGREE	AGREE	STRONGLY AGREE	SOMEWHAT LIKELY	STRONGLY AGREE	AGREE
15	STRONGLY AGREE	AGREE	STRONGLY AGREE	SOMEWHAT LIKELY	STRONGLY AGREE	AGREE
16	AGREE	AGREE	STRONGLY AGREE	LIKELY	STRONGLY AGREE	AGREE
17	AGREE	AGREE	AGREE	LIKELY	AGREE	AGREE
18	AGREE	AGREE	STRONGLY AGREE	SOMEWHAT LIKELY	STRONGLY AGREE	AGREE
19	AGREE	NEUTRAL	STRONGLY AGREE	SOMEWHAT LIKELY	STRONGLY AGREE	AGREE
20	STRONGLY AGREE	STRONGLY AGREE	STRONGLY AGREE	LIKELY	STRONGLY AGREE	STRONGLY AGREE
21	AGREE	AGREE	STRONGLY AGREE	LIKELY	STRONGLY DISAGREE	STRONGLY DISAGREE
22	STRONGLY AGREE	STRONGLY AGREE	STRONGLY AGREE	LIKELY	STRONGLY AGREE	STRONGLY AGREE
23	AGREE	STRONGLY AGREE	STRONGLY AGREE		AGREE	STRONGLY AGREE
24	STRONGLY AGREE	AGREE	STRONGLY AGREE	LIKELY	STRONGLY AGREE	STRONGLY AGREE
25	STRONGLY AGREE	AGREE	AGREE	LIKELY	AGREE	AGREE
26	STRONGLY AGREE	STRONGLY AGREE	STRONGLY AGREE	LIKELY	STRONGLY AGREE	STRONGLY AGREE
27	NEUTRAL	DISAGREE	AGREE	LIKELY	AGREE	AGREE
28	AGREE	NEUTRAL	AGREE	SOMEWHAT LIKELY	NEUTRAL	NEUTRAL
29	STRONGLY AGREE	AGREE	STRONGLY AGREE	SOMEWHAT LIKELY	STRONGLY AGREE	STRONGLY AGREE
30	STRONGLY AGREE	NEUTRAL	STRONGLY AGREE	LIKELY	STRONGLY AGREE	AGREE
31	STRONGLY AGREE	AGREE	AGREE	SOMEWHAT LIKELY	AGREE	NEUTRAL
32	NEUTRAL	NEUTRAL	NEUTRAL	UNKNOWN	NEUTRAL	NEUTRAL
33	AGREE	AGREE	AGREE	UNKNOWN	AGREE	NEUTRAL
34	STRONGLY AGREE	STRONGLY AGREE	STRONGLY AGREE	LIKELY	STRONGLY AGREE	STRONGLY AGREE
35	STRONGLY AGREE	STRONGLY AGREE	STRONGLY AGREE	LIKELY		STRONGLY AGREE
36	NEUTRAL	AGREE	STRONGLY AGREE	UNKNOWN	STRONGLY AGREE	STRONGLY AGREE

## Detailed CSP Reports

### COMPANY STATUS AT END OF ENGAGEMENT

DoD Supply Chain Client	Company now has a good idea of costs needed to gain and maintain compliance	Company has dedicated staff time allocated to cybersecurity compliance	Company has executive leadership buy-in for cybersecurity	Company understands cybersecurity risk management as a business need	Company has a business development plan to capitalize on their status as a secure/ low risk provider	Company has plan to under go a CMMC audit (when available)
1	✓		✓	✓		✓
2	✓		✓	✓		✓
3	✓	✓	✓		✓	
4	✓		✓	✓		✓
5	✓	✓	✓	✓		✓
6			✓			
7	✓		✓	✓		✓
8				✓		
9		✓		✓		✓
10	✓	✓				
11	✓	✓	✓	✓	✓	✓
12	✓		✓			
13		✓	✓	✓		✓
14	✓	✓	✓	✓	✓	✓
15				✓		
16			✓	✓		
17	✓			✓		✓
18			✓	✓		
19	✓	✓	✓	✓		✓
20	✓		✓	✓		✓
21	✓		✓	✓	✓	✓
22	✓	✓	✓	✓	✓	✓
23	✓	✓	✓	✓	✓	✓
24	✓	✓	✓	✓	✓	✓
25	✓		✓	✓	✓	✓
26	✓		✓	✓		✓
27						
28						
29	✓	✓		✓		
30	✓	✓	✓	✓	✓	✓
31	✓		✓			
32				✓		
33				✓		
34	✓		✓	✓		✓
35	✓		✓	✓		✓
36	✓	✓	✓	✓	✓	✓



**When asked what could have been done to better prepare this company to start the cybersecurity compliance process, participants responded:**

- A better understanding of scoping and options around compliance. Client only has a small handful of users that handle and create CUI which made an enclave the most cost effective implementation.
- To better prepare this company to start the cybersecurity compliance process, I believe having a better understanding about when a product or service is defined as CUI or COTS would have been extremely helpful so we know at what point the security measures need to be applied. This is essentially the key component of proper scoping. Additionally, understanding the potential impacts and risks of being non-compliant with emerging regulations, which includes a lean supply chain awareness and training and other flow down requirements.
- This company has never been audited on their flowdowns. Helping them understand contract enforcement impacts would likely motivate more action.
- More specific educational guidance on what “good” looks like in a hybrid onprem/cloud environment
- Full executive buy-in and support at an earlier period. Dedicated staff member/project manager to oversee the process. Earlier inclusion of outside subject matter experts (SMEs).
- I think this company has been ready to start a cybersecurity program. However, not having an internal IT dept or dedicated resources makes this a challenge. Additional funding from DoD / grants would be great.
- To better prepare this company to start the cybersecurity compliance process, I believe having a better understanding about when a product or service is defined as CUI or COTS would have been extremely helpful so we know at what point the security measures need to be applied. This is essentially the key component of proper scoping. Additionally, understanding the potential impacts and risks of being non-compliant with emerging regulations, which includes a lean supply chain awareness and training and other flow down requirements.
- Additional grants from DoD would be very helpful. The company is aware of the importance of cybersecurity however, if the company has not been investing into cybersecurity over the years, this initial lift is huge. Small DIBs should be eligible for perhaps, yearly grants that could be directed towards cybersecurity related projects.
- They did not take the process seriously until they were no longer allowed to process POs with their customer. Now that the accountability (SPRS) is there, it made the process easier to work through.
- Better education on CMMC compliance around Mantel’s specific technology stack. Client did not have much guidance from their Cloud provider.
- Client has been aware of DFARS/CMMC requirements for some time, but they have not progressed their compliance efforts primarily due to cost in conjunction with the indefinite deadline for their contracts to require compliance.
- This is the first step the company has taken in regard to DFARS/CMMC compliance, so they are starting from scratch. It would have been good if they’d already made some compliance program efforts prior to being assessed.
- A better understanding of the requirements and timelines around implementation of CMMC practices
- Better understanding of the costs involved with DFARS/CMMC compliance. Quite a few smaller members of the DiB don’t understand that all CMMC practices need to be put into place rather than being able to check the box with perceived compensating controls
- Better picture of what “good” looks like for smaller members of the DiB. OSC did not have a template to follow to implement security practices to lead to compliance

- Client was decently prepared. The IT Manager was very aware of CMMC and 800-171 and had other experience with compliance frameworks. Client also had a recent GAP analysis performed for 800-171 which showed that their organization had started to take interest in leveling themselves up.



### General Comments on Engagement with Company:

- The technical staff is very sharp and fun to work with. Their ownership does not appear interested in cybersecurity even if it's to his own benefit. Bridging this gap is very challenging.
- Client has a good cybersecurity stance, especially compared to their peers. They hadn't really understood the requirement for documentation
- Working with Client was a lot of fun. They started with a blank page for their cybersecurity program, they are now well on their way with policy and procedures to align themselves to CMMC level 3. Starting to build their documentation, Hobart is now also seeing a need to plan for a budget for future cybersecurity requirements.
- Working with this Client was an exciting challenge. Not from a people perspective, from a future cybersecurity perspective. The small DIBs such as this Client, have not over the years had a direct budget for cybersecurity related costs. These initial costs will be a heavy lift. Having performed this GAP analysis and working with their staff, they will be able to continue their journey towards CMMC level 3. However, the technical control cost will be a challenge.
- Client appreciates the value of IT security and understands how CMMC represents an opportunity for market differentiation. They are concerned about the cost to achieve compliance. This led them to a limited-scope enclave-based environment instead of securing their entire computing environment as they'd prefer. This isn't the DoD's or IW's fault, but it shows that DIBs are very concerned about the cost to adequately secure and certify their operations.
- Client had very specific questions about their hybrid environment including implementation of CMMC practices over the cloud provider products. We performed quite a bit of research to create a solution that would work with their current tech stack and address the gaps in their current provider.
- Client has been a customer for a number of years, but their compliance progress has been slow. That's not because of not knowing the requirements but rather committing the resources to becoming compliant.
- Prior to this engagement, Client had only heard about DFARS/CMMC. As a result, they had made no progress at the start of the engagement. Because we are so early in the process, it's hard to discern their approach for the future. Compliance represents a significant change in their operations.
- Great outcome with Client, we worked heavily with their MSP to create a template for services that are CMMC compliant
- Client was looking at CMMC compliance for future tenders and did not currently have DFARS obligations.
- Working with this Client was a great experience from the start. Our weekly meetings helped to keep us on track. The Client also has an internal full time IT manager who understood the importance however, trying to level up his companies cybersecurity posture while maintaining everything is a challenge.

# APPENDIX G

## Outreach Materials

**IMPACT WASHINGTON**  
National Network

Impact Washington is pleased to announce that it has received nearly \$1 million in grant funding to support our DoD cybersecurity consulting and training programs in Washington State. This funding will provide no-cost cybersecurity readiness training to companies in the Washington defense supply chain.

**"Our military and defense industry strengthen communities all over the state by supporting over \$13 billion in annual procurements with nearly 2,000 Washington manufacturers. This sector is vital to creating an economic climate where innovation and entrepreneurship continue to thrive," said Washington Commerce Director Lisa Brown.**

The grant award is from the U.S. Department of Defense Office of Economic Adjustment (DoD - OEA) and is supported by the Washington State Department of Commerce's Office of Economic Development and Competitiveness. The Impact Washington/Commerce collaboration hopes to reach every DoD supplier to help them understand and prepare for compliance with current DPA/NIST 800-171 cybersecurity requirements and the emerging CMMC (Cybersecurity Maturity Model Certification) standard.

Impact Washington has developed self-paced, e-learning courses that will educate defense contractors on cybersecurity requirements and provide guidance on structuring a roadmap and developing a plan to move toward compliance. In addition, no-charge in-depth consulting will be made available to 20 selected companies to provide technical assistance toward meeting these cyber requirements.

The DPA/NIST 800-171 and CMMC readiness training is offered at no cost to members of the Washington State defense supply chain. Grant funds cover your costs. Our goal is to minimize the time needed to understand these standards and facilitate the actionable steps to move toward compliance.

**The first step: pre-register for the Fall self-guided DPA/NIST 800-171 and CMMC Readiness Program. Companies that participate in the no-charge Readiness Program will be considered for additional technical assistance.**

Please contact **Impact Washington** or email [cyber@impactwashington.org](mailto:cyber@impactwashington.org) for additional information or questions. We look forward to seeing your company on the training list and supporting your team's cyber needs.

Best regards,  
Deloit R. Wolfe, Jr.

*Deloit R. Wolfe, Jr.*

President, and Center Director of Impact Washington

Thank You to Our Partners in This Effort

3303 Monte Villa Parkway, Suite 340  
Bothell, WA 98021  
[info@impactwashington.org](mailto:info@impactwashington.org)  
425.287.8808

### September 8th, 2020 Outreach Letter

### Cybersecurity Help for Washington State Defense Supply Chain Companies

**IMPACT WASHINGTON**  
National Network

Thank you for recently pre-registering for one of our CMMC Readiness Courses. We appreciate your patience while we've been preparing to launch this critical information.

These cybersecurity training courses are designed to assist the Department of Defense (DoD) suppliers (prime and subcontractors) to comply with cybersecurity requirements, including the emerging CMMC (Cybersecurity Maturity Model Certification) standard. **The courses will be available mid-October.**

This training is at no-charge thanks to a generous grant from the U.S. Department of Defense Office of Economic Adjustment (DoD - OEA), supported by the Washington State Department of Commerce and administered thru Impact Washington.

You will take the Readiness Courses thru the **Ignite Institute Learning Center**. Within the next few weeks, you will receive an email directly from them to provide the necessary details to access your account using your pre-registration information.

Once in the learning center, you can take the Senior Management Training, Practitioners Training, or both.

The Washington state military and defense industry is vital to the state of Washington. This industry strengthens communities all over the state by supporting over \$13 billion in annual procurements with nearly 2,000 Washington manufacturers. You've taken the first steps towards securing your DoD contracts and understanding the requirements around CMMC.

We encourage you to ask your supply chain members to sign-up for these no-cost courses to ensure all tiers along your supply chain understand the upcoming requirements. They can **register here**.

Please contact Impact Washington at [cyber@impactwashington.org](mailto:cyber@impactwashington.org) for additional information or questions about our Cybersecurity consulting or the upcoming CMMC Readiness training.

Best regards,  
*Deloit R. Wolfe, Jr.*

Deloit R. Wolfe, Jr.  
President and Center Director

**We could not bring you these courses without the support and involvement from these supporters**

3303 Monte Villa Parkway, Suite 340  
Bothell, WA 98021  
[info@impactwashington.org](mailto:info@impactwashington.org)  
425.287.8808

### October 8th, 2020 Outreach Letter

### Cybersecurity Maturity Model Certification (CMMC) Readiness Courses - Update

**IMPACT WASHINGTON**  
National Network

Defense Industrial Base Community -

Are you holding a federal contract, either directly or through a Prime? As SMB, are you beginning to hear more and more about Cybersecurity Maturity Model Certification (CMMC) and wondering what your next steps should be?

Unfortunately, there are still a lot of "ifs" "but's" and "maybes" when it comes to funding and costs for CMMC.

Fortunately for Washington State-based SMBs, a grant from the U.S. Department of Defense Office of Economic Adjustment (DoD - OEA), supported by the Washington State Department of Commerce is in place to help you prepare for the CMMC shift.

Currently, over 100 Defense Industrial Base subcontractors within the State have been vetted and are taking advantage of our assistance.

Don't miss your opportunity to participate.

Click the image below to listen and learn as Kate Kanapeaux from Pacific Northwest Defense Coalition (PNDC) interviews Geoff Lawrence from Impact Washington and Max Asulin of the Ignite Institute about the programs we have in place to support your business.

Additional information can be found on our website or you can reach out to [cyber@impactwashington.org](mailto:cyber@impactwashington.org)

**Apply for One-One-One Support**

**Register for No-Cost CMMC Readiness Training**

**IMPACT WASHINGTON CONTACT: CYBER@IMPACTWASHINGTON.ORG**

3303 Monte Villa Parkway, Suite 340  
Bothell, WA 98021  
[info@impactwashington.org](mailto:info@impactwashington.org)  
425.287.8808

### November 1st, 2020 Outreach Letter

### Don't Miss Your Opportunity for CMMC Support

**IMPACT WASHINGTON**  
National Network

**CMMC Readiness Courses  
Now Available  
Don't Miss Your Opportunity To Participate!**

All courses are self-paced. Upon completing the course(s), you will receive a Certificate of Completion. We encourage you to save this Certificate of Completion as evidence of ongoing education supporting your cybersecurity compliance program.

You will take the Readiness Courses thru the Ignite Institute Learning Center. Once in the learning center, you can participate in Senior Management Training, Practitioners Training, or both.

You have already pre-registered for these courses. If you need help accessing your login info please use this **Forgot Password URL**.

There is no cost to participate; however, this offer ends early 2021. Course fees are covered by a grant from the U.S. Department of Defense Office of Economic Adjustment (DoD - OEA), supported by the Washington State Department of Commerce and administered thru Impact Washington.

Please encourage your supply chain partners to sign-up for this training to ensure all tiers along your supply chain understand the upcoming requirements. They can **register here**.

Please contact Impact Washington at [cyber@impactwashington.org](mailto:cyber@impactwashington.org) for additional information or questions about our Cybersecurity consulting or the upcoming CMMC Readiness training.

Deloit R. Wolfe, Jr.

*Deloit R. Wolfe, Jr.*

Deloit R. Wolfe, Jr.  
President and Center Director

**We could not bring you these courses without the support and involvement from these supporters**

3303 Monte Villa Parkway, Suite 340  
Bothell, WA 98021  
[info@impactwashington.org](mailto:info@impactwashington.org)  
425.287.8808

### December 7th, 2020 Outreach Letter

### Cybersecurity Maturity Model Certification (CMMC) Readiness Courses - Login Reminder

## DFARS & UNDERSTANDING THE DOD'S CYBERSECURITY MATURITY MODEL (CMMC)

The Cybersecurity Maturity Model Certification (CMMC) is a new standard across the Defense Industrial Base (DIB) as a response from the Department of Defense (DoD) due to a significant amount of sensitive data compromises. CMMC will provide guidance and protection of sensitive data, such as Controlled Unclassified Information (CUI) and Federal Contract Information (FCI) through 17 domains. Each domain is composed of processes that

range from 'Performed' at Level 1 to 'Optimizing' at Level 5, and the practices range from 'Basic Cyber Hygiene' at Level 1 to 'Advanced/Progressive' at Level 5. The CMMC framework includes five certification levels based on the infrastructure's maturity and stability to support DoD sensitive information. Each level includes additional practices and processes, with each level being inclusive of lower-level practices.

## PARTICIPATE IN DOD SPONSORED TRAINING FOR DFARS AND CMMC

Impact Washington has teamed up with Ignite Institute to create CMMC Training Modules to provide participants with the tools and resources needed to self-manage and prepare for their organizations' compliance. Participants will learn the material through interactive sessions while having the ability to join into a larger pool of candidates looking to create roadmaps, track milestones and control the entire process for managing compliance and cybersecurity for their organization.

**REGISTER  
FOR TRAINING [HERE](#)**

For more information about Impact Washington Cybersecurity Consulting and Training Contact:

[cyber@impactwashington.org](mailto:cyber@impactwashington.org)  
425-438-1126



## WHAT CMMC WILL REQUIRE

While DFARS is the current standard, CMMC will require DoD contractors to become CMMC certified. This new standard will include all suppliers at all tiers along the supply chain, small businesses, commercial item contractors, and foreign suppliers.

### CUI Data Protection

CUI is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. Through the CMMC maturity levels, one of the main goals of the CMMC is to safeguard CUI for DoD contractors and organizations.

### Development of System Security Plan Documentation

Developing and implementing a System Security Plan (SSP) is crucial for DFARS and future CMMC compliance. It documents the people, technology, and processes related to the CUI environment. This document is a “living” document and will continually be updated as the CUI environment changes. The SSP is also a central document for the NIST 800-171 controls and acts as a “repository” for the CUI environment. The SSP will be required and will be asked for by a CMMC Auditor.

### Internal Cybersecurity Program

The CMMC Accreditation Board (AB) establishes and oversees a qualified, trained, and high-fidelity community of assessors that can deliver consistent and informative assessments to participating organizations against a defined set of controls/best practices within the CMMC Program.

### External Audit & Certification

The CMMC AB, a non-profit, independent organization, will accredit CMMC Third Party Assessment Organizations (C3PAOs) and individual assessors. Only C3PAOs and individual assessors that have been accredited by the CMMC AB will perform CMMC assessments.



## DFARS & UNDERSTANDING THE DOD'S CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

While DFARS standards and NIST 800-171 are the current DoD cybersecurity domain requirements, CMMC will require DoD contractors to become certified to the emerging CMMC standard. The CMMC standard will apply to all suppliers at all tiers along the supply chain, small businesses, commercial item contractors, and foreign suppliers.

CMMC is a unified cybersecurity standard for implementing cybersecurity across the entire defense supply chain and is the DoD's response to significant compromises of sensitive defense information located on contractors' information systems. The CMMC establishes five certification levels that reflect the maturity and reliability of a company's cybersecurity infrastructure to safeguard sensitive government information on contractors' information systems.

CMMC compliance will soon be the minimum requirement to be eligible for DoD contract awards. Moreover, the DoD has emphasized that the CMMC is a starting point for transforming contractors' internal cybersecurity culture.

Impact Washington is offering no-cost DFARS and NIST 800-171 and CMMC training to members of the Washington State defense supply chain. This training is in the form of digital, self-paced courses tailored to a defense contractor, from the CEO, to operations

& financial managers to Engineering & IT professionals.

Participants will be able to customize their course work by selecting modules that directly apply to their responsibilities and the organization's needs.

### Two separate courses are available:

- ✓ The senior management course focuses on the importance of cybersecurity in protecting company assets and resources and outlining the measures and resources needed to achieve compliance.
- ✓ The practitioner course facilitates and identifies the steps needed to move the company toward DFARS and CMMC compliance.

These CMMC courses are the beginning of establishing a CMMC pathway to achieve your desired level of cybersecurity maturity and succeed as a DoD contractor or subcontractor.



# DFARS & UNDERSTANDING THE DOD'S CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

## FOR SENIOR MANAGEMENT

### About this course:

This course provides a general overview of the DFARS standards and NIST 800-171 and how they relate to emerging CMMC compliance requirements. Participants will go through the origins of CMMC, its essential core components, and what the DoD will expect. This path will also illustrate that in addition to technical requirements, much of CMMC compliance is non-technical and involves the implementation of cybersecurity best practices. The course will enable you to think critically about the importance of cybersecurity, recognize its place in your company's risk management strategy, and visualize a path to achieve compliance.

### Who Should Attend:

CEOs, Procurement Specialists, and Senior managers with legal, financial, and compliance responsibilities.

### What you will learn:

- ✓ Compare the DFARS standards, NIST 800-171, and the CMMC domain requirements.
- ✓ Interpret barriers and challenges of cybersecurity compliance.
- ✓ Communicate the steps and resources required in the CMMC readiness process.
- ✓ Connect sources of support to achieve DFARS and CMMC compliance.
- ✓ Determine a path for DFARS and CMMC audit readiness.

### Length:

20 minutes (self-paced)

### Training Completion Document:

Upon course completion

[Register for Training Here](#)

## FOR PRACTITIONERS

### About this course:

This course will unpack the alignment of the DFARS standards and NIST 800-171 with the 5 levels of CMMC, focusing on level 3. Modules will illustrate the process for implementing all the required standards and practices for DoD compliance, and provide guidance, resources, and tools for preparing and submitting a CMMC certification package.

### Who Should Attend:

Operations managers, HR professionals, Engineering/IT, and other technical personnel.

### Length:

40-60 minutes (Self-paced instruction + additional time for the Toolbox)

### Training Completion Document:

Upon course completion

### What you will learn:

- ✓ Assess your current and future contracts to DFARS standards, NIST 800-171 and emerging CMMC requirements.

- ✓ Evaluate your current cybersecurity processes and practices against DFARS, NIST 800-171 and the emerging CMMC level requirements.
- ✓ Establish and implement a gap analysis between your current processes & practices, and DFARS, NIST 800-171 and CMMC standards.
- ✓ Review, draft, and revise your system security plan to meet DFARS standards, NIST 800-171 and establish a pathway to CMMC compliance.

### Toolbox:

CMMC Training Modules provide participants with the tools and resources to self-manage and progress toward their organization's compliance. Participants will learn CMMC material through interactive sessions while having the ability to join into a larger pool of candidates. These tools will enable participants to create roadmaps, track milestones, and control the entire process to manage cybersecurity and move toward compliance.

[Register for Training Here](#)

## OUTREACH MATERIALS

### August 14, 2020 - Press Release



#### Washington State Department of Commerce Invests in Defense Manufacturers with Cybersecurity Training

*Partnership with Impact Washington will provide Defense Manufacturers with actionable steps to comply with emerging cybersecurity standards.*

**Bothell, WA (August 14, 2020)** – Today, [Deloit R. Wolfe Jr.](#), President, and Center Director of Impact Washington, announced that Impact Washington would receive nearly \$1 million in grant funding for the firms' DoD cybersecurity consulting and training programs.

The grant is from the U.S. Department of Defense Office of Economic Adjustment (DoD - OEA), supported by the Washington State Department of Commerce. This partnership between Commerce's Office of Economic Development and Competitiveness and Impact Washington proposes a unique collaboration to provide awareness and training to companies with DoD contracts throughout the state.

While DFARS and NIST 800-171 are current standards, the emerging CMMC will require DoD contractors to become CMMC certified. This will include all suppliers at all tiers along the supply chain, small businesses, commercial item contractors, and foreign suppliers. For contracts that require CMMC, certification will be required for consideration.

"Our military and defense industry strengthens communities all over the state by supporting over \$13 billion in annual procurements with nearly 2,000 Washington manufacturers. This sector is vital to creating an economic climate where innovation and entrepreneurship continue to thrive," said Washington Commerce Director Lisa Brown. "Impact Washington is an ideal partner to help our state's manufacturing firms and their supply chains prepare for new certifications that will be required to continue serving the DoD."

Wolfe commented, "Impact Washington is committed to supporting the defense workforce and contractors throughout the state. Cybersecurity compliance awareness and training designed for defense contractors and their supply chains to address the ever-growing threat of cyberattacks is needed as the federal compliance date draws near. Grants like these enable us to support investments in developing curriculum, training, and outreach programs that minimize a manufacturer's time in understanding the changes and the actionable steps to comply with these emerging standards."

For more information Impact Washington's DoD Cybersecurity consulting and DFARS-CMMC Readiness training program visit [www.impactwashington.org](http://www.impactwashington.org).

#### About Impact Washington

Impact Washington is a statewide non-profit organization that provides competitive, value-driven services. With access to public and private resources, our goal is to enhance growth, improve productivity, reduce costs, and expand

3303 Monte Villa Parkway, Suite 340 Bothell, WA 98021  
425.438.1146 | [impactwashington.org](http://impactwashington.org)