

Welcome to the 2020 Industry Resilience Virtual Convening

- All attendees are in listen only mode.
- Attendees can submit questions to our presenters anytime during the webinar by using the questions box you will find in your gotowebinar interface.
- The webinar is being recorded and recordings for all the sessions will be emailed out to all registrants on Friday, May 8th

2020

OEA Industry Resilience Learning
Community Exchange: Virtual
Convening Webinar 4



Cybersecurity: CMMC Update and What's Next?

May 7, 2020



Paul Shaw

- Professor, Cybersecurity
- Defense Acquisition University
- 619-591-9736
- 619-869-6761
- Paul.Shaw@dau.edu





Corbin Evans

- Director of Strategic Programs
- National Defense Industrial Association
- (703) 247 – 2598
- CEvans@NDIA.org

NDIA

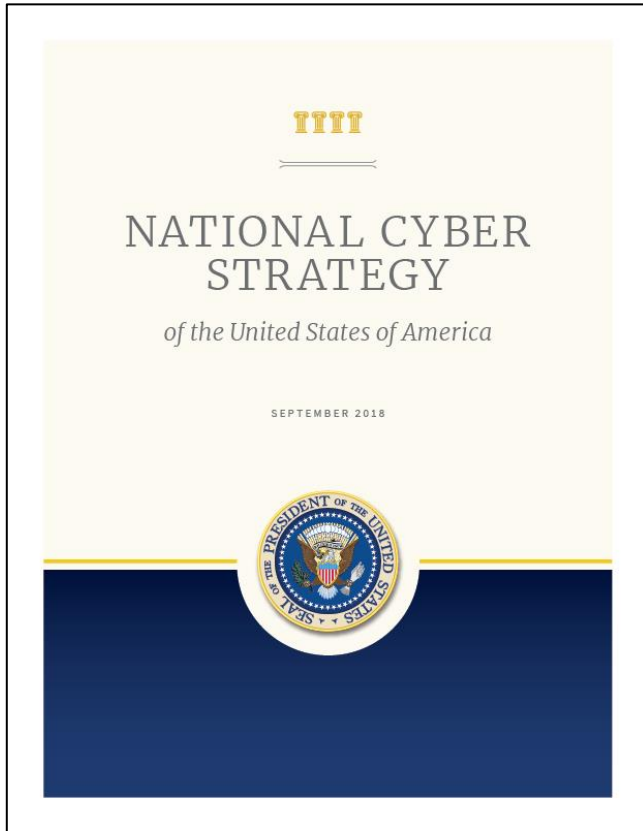


Gordon Bitko

- Senior Vice President, Public Sector
- Information Technology Industry Council
- 310-923-0824
- gbitko@itic.org



National Cyber Strategy



STRENGTHEN FEDERAL CONTRACTOR CYBERSECURITY:

“The United States cannot afford to have sensitive government information or systems inadequately secured by contractors. Federal contractors provide important services to the United States Government and must properly secure the systems through which they provide those services. Going forward, the Federal Government will be able to assess the security of its data by reviewing contractor risk management practices and adequately testing, hunting, sensing, and responding to incidents on contractor systems. Contracts with Federal departments and agencies will be drafted to authorize such activities for the purpose of improving cybersecurity. Among the acute concerns in this area are those contractors within the defense industrial base responsible for researching and developing key systems fielded by the DOD.” (p. 7)

Cybersecurity in Africa

Is your Security Team – just downloading a Template?

Do you defend against Opportunistic Attack or Worst Case Attack?

You know the cost difference between Opportunistic Attack & Worst Case Attack?

Security Team knows what to change – if the threat changes?

How do you determine & measure value for your security activities?

How would you answer listed key questions?

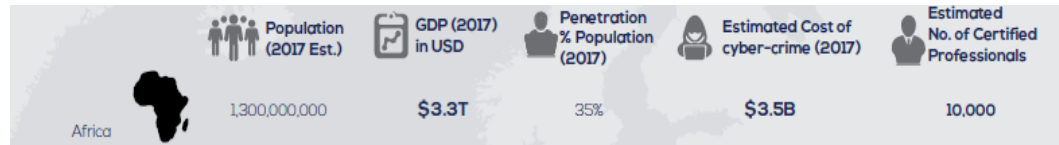
Skill gap: What you do not know will hurt you

The cost of Cybercrime grew by approximately 20% but the skill gap is widening. Very few people know what they're doing, most IT and security staff are downloading templates from the internet and applying these in their organisations. From our analysis, a key contributor to this is that organisations tend to look for people with traditional technology credentials – IT, Computer Science. But when you look at the matter, we need Technology analysts, Cyber Risk Engineers, data analysts, Risk experts most of which do not necessarily warrant a technology course. Majority of organisations encourage their IT teams to take up courses that don't necessarily add value to the security of the organisations.

It is also concerning that companies would rather poach talent from each other and from training providers than develop it themselves.

This points to the sad fact that businesses are thinking in the short term. Rather than cultivating the needed talent, organisations are continuously relying on ready-made talent pool.

(p. 16)



<https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf>

What does the future hold for this problem?

As cyber-attacks continue to evolve, it's paramount that organisations rise above the cyber security poverty line. In a world where buying a tool is considered a silver bullet to solving cyber security issues, it's critical that we ask ourselves key questions:

- What are my organisations top risks?
- What is the worst that can happen to my business?
- What do I need to do to ensure that I have secured my systems against these threats?

(p. 10)

Cybersecurity Poverty Line



What is the cyber security poverty line?

Many organisations particularly SMEs lack the basic "commodities" that would assure them of the minimum security required and with the same analogy, be considered poor.

In the context of a cyber-security poverty line there are still numerous organisations particularly SMEs that do not have the skills, resources or funding to protect, detect and respond to cyber security threats. Many organisations and individuals fall below this line. We aim to demystify the cyber security poverty line within Africa.

(p. 9)



- Africa > 90% Below Poverty Line
- How many Small DoD Contractors would be below the Cybersecurity Poverty Line?

General characteristics of organisations operating below the Cyber security poverty line are:

- Lack the minimum requirement for fending off an opportunistic adversary. → **Vulnerable to Opportunistic Attacker**
- Are essentially waiting to get taken down by an attack. → **Reactive response to attacks**
- There's also the idea of technical debt as a result of postponing important system updates. → **Postpones System Updates**
- Lack in-house expertise to maintain a decent level of security controls and monitoring → **Lacks Expertise to maintain security controls**
- Tremendously dependent on third parties hence have less direct control over the security of the systems they use. → **Dependent upon 3rd Parties for security**
- They also end up relinquishing risk decisions to third parties that they ideally should be making themselves. → **Relinquishes Risk Decisions to 3rd Parties**
- Lack resources to implement separate systems for different tasks, or different personnel to achieve segregation of duties. → **Lacks Segmentation of Duties**
- They'll use the cheapest software they can find regardless of its quality or security. → **Uses cheapest SW, Regardless of security**
- They'll have all sorts of back doors to make administration easier for whoever they can convince to do it. → **Allows back doors to easy Administrator tasks**

(p. 10)

Cybersecurity in Africa

Africa has created a Threat Dividing Line

- Opportunistic Attacker
 - Worst Case Attacker
-
- Everyone should be capable of defending against an Opportunistic Attacker
 - Unable to defend against an Opportunistic Attacker - below the Poverty Line
 - Progressive organizations can change & defend against a range of threats

DoD Contractor Cybersecurity

FY 20 NDAA Section 1648 requires the Secretary of Defense to develop a comprehensive framework to enhance the cybersecurity of the U.S. defense industrial base no later than February 1, 2020.

What are the potential cybersecurity standards, regulations, metrics, ratings, and third-party certifications that prime contractors/ subcontractors must meet to successfully implement the current DFARS Clause 252.204-7012 and future Cybersecurity Maturity Model Certification (CMMC) initiative.

FY20 NDAA Sec 1648 Key Provisions

- A framework to protect sensitive unclassified DoD information under the control of a DoD Contractor
- Applicable to the Prime Contractor & their Supply Chain
- Implementation is a Risk-based Approach & Tailorable
- Contractor & their supply chain compliance will be assessed through certification (future) & DoD oversight
- Cyber Threat Information needs to be communicated to DoD Contractors & their Supply Chain
- Enhanced security requirements could apply – in accordance with the Cyber Threat

FY20 NDAA

One Hundred Sixteenth Congress of the United States of America

AT THE FIRST SESSION

*Begun and held at the City of Washington on Thursday,
the third day of January, two thousand and nineteen*

An Act

To authorize appropriations for fiscal year 2020 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

*Be it enacted by the Senate and House of Representatives of
the United States of America in Congress assembled,*

SECTION 1. SHORT TITLE.

This Act may be cited as the “National Defense Authorization Act for Fiscal Year 2020”.

SEC. 1648. FRAMEWORK TO ENHANCE CYBERSECURITY OF THE UNITED STATES DEFENSE INDUSTRIAL BASE. (pp. 1410 - 1413)

(a) FRAMEWORK REQUIRED.—Not later than February 1, 2020, the Secretary of Defense shall develop a consistent, comprehensive framework to enhance cybersecurity for the United States defense industrial base.

(b) ELEMENTS.—The framework developed pursuant to subsection (a) shall include the following:

(1) Identification of unified cybersecurity standards, regulations, metrics, ratings, third-party certifications, or requirements to be imposed on the defense industrial base for the purpose of assessing the cybersecurity of individual contractors.

....

(3) The responsibilities of the prime contractors, and all subcontractors in the supply chain, for implementing the required cybersecurity standards, regulations, metrics, ratings, third-party certifications, and requirements identified under paragraph (1).

(4) Definitions for “Controlled Unclassified Information” (CUI) and “For Official Use Only” (FOUO), as well as policies regarding protecting information designated as either of such.

(5) Methods and programs for managing controlled unclassified information, and for limiting the presence of unnecessary sensitive information on contractor networks.

(6) A plan to provide implementation guidance, education, manuals, and, as necessary, direct technical support or assistance, to contractors on matters relating to cybersecurity.

(7) Quantitative metrics for assessing the effectiveness of the overall framework over time, with respect to the exfiltration of controlled unclassified information from the defense industrial base.

(8) A comprehensive list of current and planned Department of Defense programs to assist the defense industrial base with cybersecurity compliance requirements of the Department, including those programs that provide training, expertise, and funding, and maintain approved security products lists and approved providers lists.

(9) Processes for enhanced threat information sharing between the Department of Defense and the defense industrial base.

FY20 NDAA Sec 1648

SEC. 1648. FRAMEWORK TO ENHANCE CYBERSECURITY OF THE UNITED STATES DEFENSE INDUSTRIAL BASE. (pp. 1410 - 1413)

(c) MATTERS FOR CONSIDERATION.—In developing the framework pursuant to subsection (a), the Secretary shall consider the following:

- ...(2) Risk-based methodologies, standards, metrics, and tiered cybersecurity requirements for the defense industrial base, including third-party certifications such as the Cybersecurity Maturity Model Certification pilot program, as the basis for a mandatory Department standard.
- (3) Tailoring cybersecurity requirements for small- and medium-sized contractors based on a risk-based approach.
- (4) Ensuring a consistent approach across the Department to cybersecurity standards, regulations, metrics, ratings, third-party certifications, or requirements of the defense industrial base.
- (5) Ensuring the Department's traceability and visibility of cybersecurity compliance of suppliers to all levels of the supply chain.
- (6) Evaluating incentives and penalties for cybersecurity performance of suppliers.
- ...
- (8) Establishing a secure software development environment (DevSecOps) in a cloud environment inside the perimeter of the Department for contractors to perform their development work.
- (9) Establishing a secure cloud environment through which contractors may access the data of the Department needed for their contract work.

(10) An evaluation of the resources and utilization of Department programs to assist the defense industrial base in complying with cybersecurity compliance requirements referred to in subsection (b)(1).

(11) Technological means, operational concepts, reference architectures, offensive counterintelligence operation concepts, and plans for operationalization to complicate adversary espionage, including operation concepts, and plans for operationalization to complicate adversary espionage, including honeypotting and data obfuscation.

(12) Implementing enhanced security vulnerability assessments for contractors working on critical acquisition programs, technologies, manufacturing capabilities, and research areas.

(13) Identifying ways to better leverage technology and employ machine learning or artificial intelligence capabilities, such as Internet Protocol monitoring and data integrity capabilities, to be applied to contractor information systems that host, receive, or transmit controlled unclassified information.

(14) Developing tools to easily segregate program data to only allow subcontractors access to their specific information.

(15) Appropriate communications of threat assessments of the defense industrial base to the acquisition workforce at all classification levels.

...

(17) Appropriate communications with the defense industrial base on the impact of cybersecurity requirements in contracting and procurement decisions.

What is the Difference in These Threat Capabilities



Office of the Under Secretary of Defense for
Acquisition & Sustainment
Cybersecurity Maturity Model Certification

	Description of Practices
Level 1	<ul style="list-style-type: none"> Basic cybersecurity Achievable for small companies Subset of universally accepted common practices Limited resistance against data exfiltration Limited resilience against malicious actions
Level 2	<ul style="list-style-type: none"> Inclusive of universally accepted cyber security best practices Resilient against <u>unskilled threat actors</u> ← Minor resistance against data exfiltration Minor resilience against malicious actions
Level 3	<ul style="list-style-type: none"> Coverage of all NIST SP 800-171 rev 1 controls Additional practices beyond the scope of CUI protection Resilient against <u>moderately skilled threat actors</u> ← Moderate resistance against data exfiltration Moderate resilience against malicious actions Comprehensive knowledge of cyber assets
Level 4	<ul style="list-style-type: none"> Advanced and sophisticated cybersecurity practices Resilient against <u>advanced threat actors</u> ← Defensive responses approach machine speed Increased resistance against and detection of data exfiltration Complete and continuous knowledge of cyber assets
Level 5	<ul style="list-style-type: none"> Highly advanced cybersecurity practices Reserved for the most critical systems Resilient against the <u>most-advanced threat actors</u> ← Defensive responses performed at machine speed Machine performed analytics and defensive actions Resistant against, and detection of, data exfiltration Autonomous knowledge of cyber assets

CMMC has four levels of threat actors:

- Unskilled Threat Actor
- Moderately Skilled Threat Actor
- Advanced Threat Actor
- Most-advanced Threat Actor

What are the differences in capabilities across these threat actors to act as a(n):

- External Attacker
- Insider Threat
- Supply Chain Attacker

<https://www.acq.osd.mil/cmmc/faq.html>


DFARS Clause 252.204-7012

- Resource: *Guidance to Stakeholders for Implementing Defense Federal Acquisition Regulation Supplement Clause 252.204-7012 (Safeguarding Unclassified Controlled Technical Information)*
- Basic Supplier Requirements:
 - **Provide adequate security - DFARS 252.204-7012(b)**
 - **Report cyber incidents - DFARS 252.204-7012(c)**
 - **Flow down these requirements - DFARS 252.204-7012(m)**

**Note: Adequate Security =
Implementing NIST 800-171 Rev 1 Security Requirements**

Potential Impact

“With regard to *federal information systems*, requirements in the federal regulation for protecting CUI at the moderate confidentiality impact level will be based on applicable policies established by OMB and applicable government wide standards and guidelines issued by NIST.” NIST 171 r1, p. v

	POTENTIAL IMPACT		
Security Objective	LOW	 MODERATE	HIGH
<i>Confidentiality</i> Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

FIPS 199, p. 6

NIST 800 -171A Assessing Security Requirements

NIST Special Publication 800-171A

Assessing Security Requirements for Controlled Unclassified Information

RON ROSS
KELLEY DEMPSEY
VICTORIA PILLITTERI

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

The information gathered and the evidence produced can be used by an organization to:

- Identify potential problems or shortfalls in the organization's security and risk management programs;
- Identify security weaknesses and deficiencies in its systems and in the environments in which those systems operate;
- Prioritize risk mitigation decisions and activities;
- Confirm that identified security weaknesses and deficiencies in the system and in the environment of operation have been addressed; and
- Support continuous monitoring activities and provide information security situational awareness.

Protecting Unclassified CTI

Guidance to Stakeholders for Implementing
Defense Federal Acquisition Regulation Supplement
Clause 252.204-7012
(Safeguarding Unclassified Controlled
Technical Information)



Version 2.0

August 2015

Office of the Deputy Assistant Secretary of Defense for Systems Engineering
Washington, D.C.

Distribution Statement A: Approved for public release.

Q: Who is responsible for identifying/marketing unclassified CTI?

A: The controlling DoD office (defined in DoDI 5230.24), in most cases the requiring activity, is responsible to:

- 1) Determine whether the relevant technical information to be furnished by the Government and/or developed by the contractor contains unclassified CTI. The requiring activity must notify the procuring contracting officer (PCO) when a potential contractor will be required to develop and/or handle unclassified CTI.
- 2) Review all unclassified CTI to be provided to the contractor to verify that all document distribution statements are valid and that all documents that should be marked are properly marked with the correct statement prior to their being provided to the contractor.

DoDI 5200.48 Controlled Unclassified information



DoD INSTRUCTION 5200.48

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

Originating Component:	Office of the Under Secretary of Defense for Intelligence and Security
Effective:	March 6, 2020
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whis.mil/DD/ .
Cancels:	DoD Manual 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information," February 24, 2012, as amended
Approved by:	Joseph D. Keran, Under Secretary of Defense for Intelligence and Security (USD(I&S))

Purpose: In accordance with the authority in DoD Directive (DoDD) 5143.01 and the December 22, 2010 Deputy Secretary of Defense Memorandum, this issuance:

- Establishes policy, assigns responsibilities, and prescribes procedures for CUI throughout the DoD in accordance with Executive Order (E.O.) 13556; Part 2002 of Title 32, Code of Federal Regulations (CFR); and Defense Federal Acquisition Regulation Supplement (DFARS) Sections 252.204-7008 and 252.204-7012.
- Establishes the official DoD CUI Registry.

"Pursuant to section 252.204-7012 of the DFARS, scientific, technical, and engineering information beyond basic research ... shall be treated as CUI. This type of information or data can become classified by compilation or aggregation ... Examples include preliminary research and engineering data, engineering drawings, and associated specifications, lists, standards, process sheets, manuals, technical reports, technical orders, studies and analyses on topics requested by DoD Components, catalog-item identifications, data sets, and computer software with executable or source code." (p. 20)

..."Non-DoD information systems processing, storing, or transmitting CUI will provide adequate security, and the appropriate requirements must be incorporated into all contacts, grants, and other legal agreements with non-DoD entities in accordance with DoDI 8582.01. The NIST SP 800-171 governs and protects CUI on non-Federal IS when applied by contract." (p. 25)

Dated 6 March 2020

DOD's CMMC



<https://www.acq.osd.mil/cmmc/faq.html>

5 - Why is the CMMC being created?

DOD is planning to migrate to the new CMMC framework in order to assess and enhance the cybersecurity posture of the Defense Industrial Base (DIB). The CMMC is intended to serve as a verification mechanism to ensure appropriate levels of cybersecurity practices and processes are in place to ensure basic cyber hygiene as well as protect controlled unclassified information (CUI) that resides on the Department's industry partners' networks.

Note: The CMMC Website and FY 20 NDAA Sec 1648 describe CMMC as a framework.

“The intent of the CMMC is to combine various cybersecurity control standards such as NIST SP 800-171, NIST SP 800-53, ISO 27001, ISO 27032, AIA NAS9933 and others into one unified standard for cybersecurity. In addition to cybersecurity control standards, the CMMC will also measure the maturity of a company's institutionalization of cybersecurity practices and processes.”

DOD's CMMC AB

<https://www.cmmcab.org/>

"Below is some guidance for those who think they are going to be assessors, and especially for defense contractors, the don'ts. Careful of what you hear and the promises being made before the official release of the CMMC.

Do's

1. When mentioning CMMC, always place the word DRAFT in front of it, so as not to mislead readers that the standard is complete and released.
2. Share valid information about the CMMC standard acquired from this site or the Official DoD site located at <https://www.acq.osd.mil/cmmc/index.html>.
3. Prepare your clients for CMMC by training and educating them for DFARS regulations and NIST 800-171 guidance. It is the law and there is an increasing number of audits being performed right now, in 2020.
4. Become an expert on CMMC by reading the standard, assessment guidance, and training materials that will be published on <https://www.acq.osd.mil/cmmc/index.html>. These materials ARE NOT YET AVAILABLE as the standard is not complete and released. Familiarize now. Actively prep later.



Home The CMMC Standard FAQ Glossary (draft) Stakeholders
Board of Directors

CMMC

(Cybersecurity Maturity Model Certification)
Accreditation Body

CMMC Information



ASSESSORS
With more than 350,000 vendors in the supply chain to the DoD, each of which will need to be assessed, we need people who are ready to make a difference. Whether you have the [Read more...](#)



C3PAO's
C3PAO's, Certified Third-Party Assessment Organizations, are the organizations where licensed assessors will come together hone their skills and [Read more...](#)



TRAINERS
In order to field a cadre of 10,000 or more professional assessors, the CMMC-AB will need trainers to educate and ensure that the CMMC standard is uniformly applied. [Read more...](#)



STAFF
The CMMC-AB was formed in January, 2020. We are building an organization from the ground up that will lead the nation and the world in the cyber arena. [Read more...](#)

Don'ts

1. Do not state that you are an expert on CMMC. You are not. The standard is not yet released. No trainer nor educator is currently accredited. No certified training exists yet.
2. Currently, DFARS regulation requires self-assessments under NIST 800-171 guidance. Do not focus training on future requirements (CMMC) at the expense of current requirements.
3. Do not charge clients for workshops, seminars, and training that promise CMMC compliance. The CMMC-AB will provide training and certifications to empower you with those opportunities.
4. Do not sell or promote tools that promise CMMC compliance with certainty. The CMMC-AB will create standards for tool producers to use. For now, ensure that any tools promoted focus first on completed and released standards, or best practices."

DOD's CMMC AB

<https://www.cmmcab.org/>

“Since I introduced the Cybersecurity Maturity Model Certification model last year, I have consistently stressed the importance of communicating and engaging extensively with industry, academia, military services, the Hill and the public to hear their concerns and suggestions. The purpose of this communication was, and still is, to ensure everyone fully understands the intent, process and requirements of CMMC to fight the very real threats that drive us to require rigorous cybersecurity.”



“Unfortunately, the Department has learned that some third-party entities have made public representations of being able to provide CMMC certifications to enable contracting with DoD. The requirements for becoming a CMMC third-party assessment organization (C3PAO) have not yet been finalized, so it is disappointing that some are trying to mislead our valued business partners. To be clear, there are no third-party entities at this time who are capable of providing a CMMC certification that will be accepted by the Department. At this time, only training materials or presentations provided by the Department will reflect our official position with respect to the CMMC program. I have also reached out to the presidents of the PSC, AIA and NDIA industry associations to make them aware as well, and they remain connected with my CMMC team.”

Industry & CMMC

- CMMC will be a requirement for all DOD contractors (Primes & Subs)
- Most contractors will be:
 - Level 1 – don't handle any Covered Unclassified Information (CUI), or
 - Level 3 – handle some CUI
- All DOD contracts will require CMMC certification by 2026

What should industry do today?

- Ensure compliance with DFARS 7012 – implement the NIST 171 controls
- Start conversation with your supply chain
- Learn about CMMC requirements
- 10 Contracts will contain CMMC in 2020 (likely in the missile defense area)

What questions remain?

- Will COVID-19 impact implementation timeline?
- How will required CMMC levels be determined?
- What is the process for determining CUI?
- How will cost be allocated?
- When will the CMMC AB be certifying assessors?

What questions remain?

- Can you re-use existing accreditations?
 - Will the AB establish reference models?
- How will information flow be handled?
- How will requirements consistency be ensured across DoD?
- How will accreditors set priorities?
- How will assessment findings be communicated, and risks managed?

Intermission

- The next portion of the webinar will start at 4:15 PM EDT
- As a reminder all attendees are in listen-only mode.
- You can submit a question at any time by using the questions box located in the gotowebinar interface.
- All recordings will be emailed out to all registrants on Friday, May 8th

2020

OEA Industry Resilience Learning
Community Exchange:
Virtual Convening



Cybersecurity Lessons from Effective Programs



Defense Cybersecurity
Assurance Program

May 7, 2020

Ashlee Breitner



- Senior Project Manager
- Economic Growth Institute at the University of Michigan
- (734)998-6614 (office)
- (734)239-1875 (cell)
- abreitn@umich.edu



**ECONOMIC
GROWTH
INSTITUTE**

UNIVERSITY OF MICHIGAN

What was DCAP 1.0?



93

Companies Compliant to DFARS



\$2.57B SALES REPRESENTED
7,085 JOBS IMPACTED



THE OHIO STATE UNIVERSITY



ECONOMIC GROWTH INSTITUTE
UNIVERSITY OF MICHIGAN

PURDUE
UNIVERSITY

DCAP-Company Eligibility Criteria



Company has operations in MI, OH or IN

And

Is a small to medium-size company

And

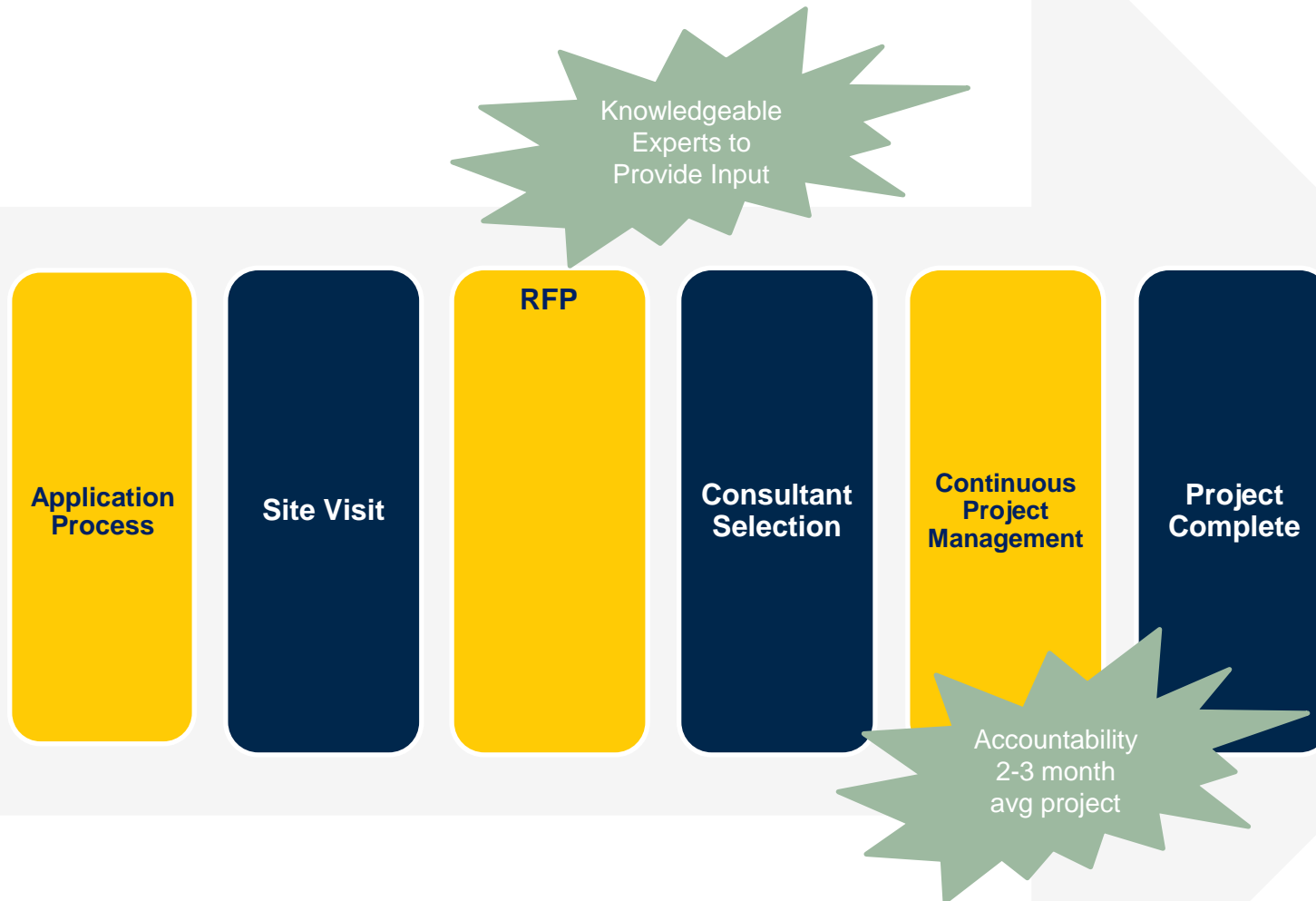
Is earning at least 10% annually of their business revenues from DoD-derived contracts (at any supply chain tier) currently or within the past 5 years.

OR

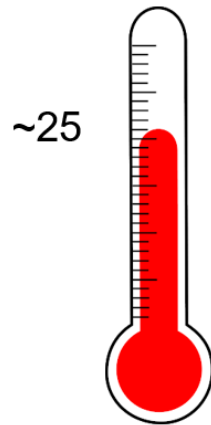
Demonstrates the critical potential to address a particular need in the defense supply chain.

Priority given to companies in rural areas.

DCAP Process



Company Assistance Projects



Educational Seminars

- Macomb, Michigan March 17, 2020
 - Traverse City, Michigan April 8, 2020
 - Muskegon, Michigan April 29, 2020
 - Jackson, Michigan May 27, 2020
 - Frankenmuth, Michigan June 10, 2020
-
- Bloomington, Indiana Nov 12, 2019
 - Fort Wayne, Indiana May 12, 2020
 - Lima, OH TBD
 - TBD, OH TBD

DCAP 2.0



Workforce Needs Focus Groups

Cyber
Technologies

Cyber
Providers

Supply Chain Mapping

Keys to Program Success

- Do what is right for the company
 - Try to simplify not scare
 - Find the BEST resources to meet the company's needs
 - Minimize costs
- Great partners
 - Universities
 - Consultants
 - Eco-system Resources (PTAC, DoL, MEP...)

"The DCAP grant combined with the program management expertise of the Economic Growth Institute at the University of Michigan took what looked like a complicated, expensive and long drawn out process and distilled it down to a well-managed and delegated process. We would not have been successful trying to implement this on our own. We are grateful for the opportunity to have been a recipient of the DCAP grant."
Bruce Barron, President and CEO of Barron Industries

Challenges Encountered

- Consultants not taking a risk based approach
- The need to pivot from self-attestation to certification

Key Lesson Learned



COVID-19's Impact on DCAP2

- Pivoting seminars to virtual or rescheduling
- Extending company project contracts due dates

Thank You!

Ashlee Breitner
abreitn@umich.edu

2020

U.S. Department of Defense OEA Industry Resilience *Virtual Convening*



Cybersecurity Lessons from Effective Programs

CASCADE

May 7, 2020





Eileen Sánchez

- CASCADE Program Director & Chief, Defense Industry Cybersecurity Resilience & Innovation
- Military Affairs, CA Governor's Office of Planning & Research
- Eileen.Sanchez@opr.ca.gov



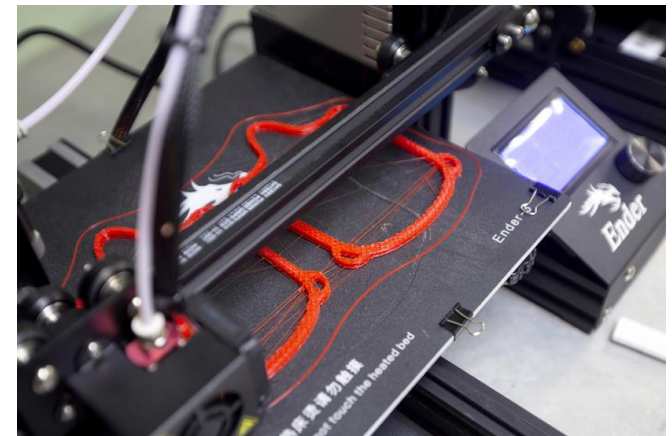
Key Take-Aways

- What are we most proud of?
- What has worked really well?
- What is our biggest challenge?
- What hasn't worked well?
- One “key lessons learned” for others considering similar work?
- How we are pivoting as a result of COVID-19?

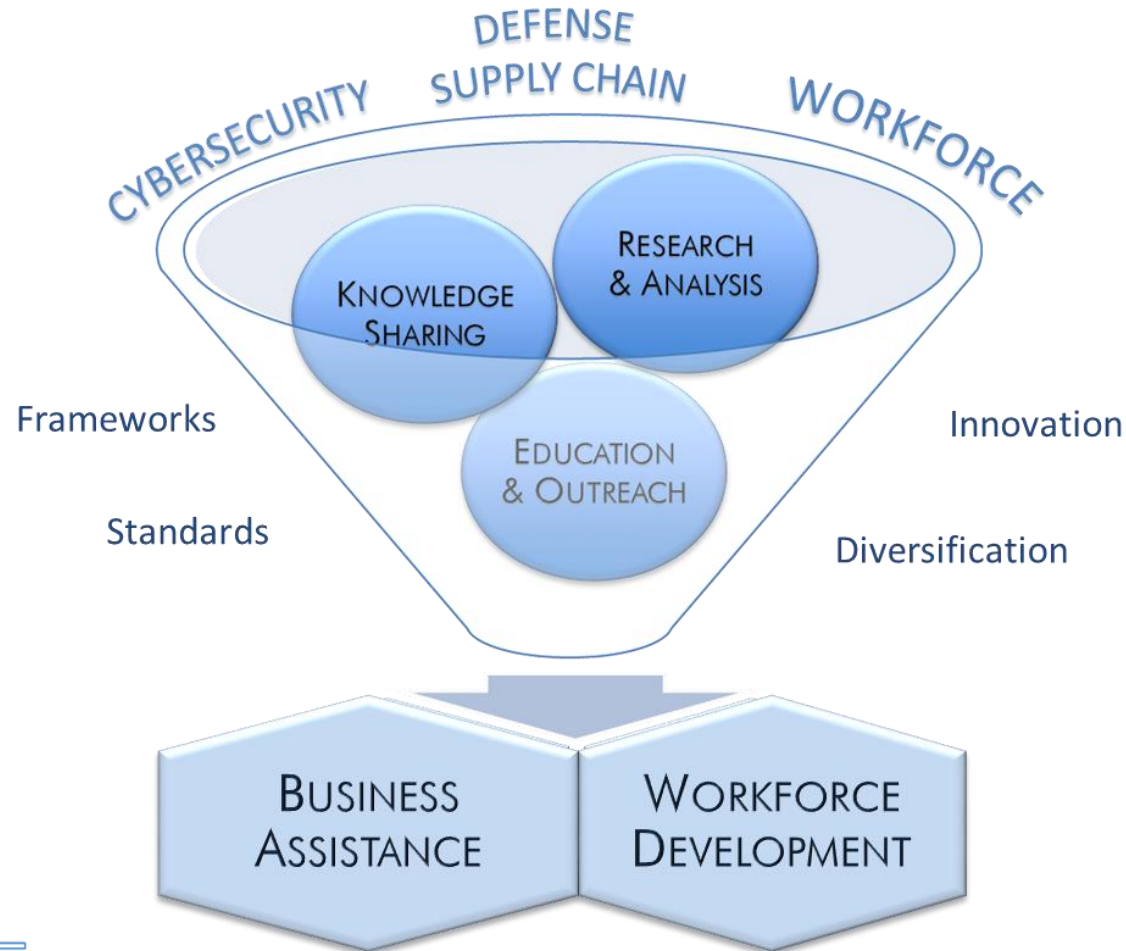


Pivoting as a result of COVID-19

- What is result of COVID19 thus far to DoD & DIB?
Threats to DoD & DIB
 - Supply chain
 - External
 - Internal
- How do you pivot?
 - Business assistance
 - Workforce development
 - Expanded partnerships



Overview of CASCADE



CASCADE I - Projects by Deliverable Category



Supporting DoD's Readiness & Modernization Priorities

Cybersecurity
Labor Market
Analysis

Cyber Provider
Mapping

Regional
Resilience
Workshops &
Resource Fairs

Cybersecurity
Bootcamps

Cybersecurity
Assessments

Strategic Alignment & Cross-Collaboration

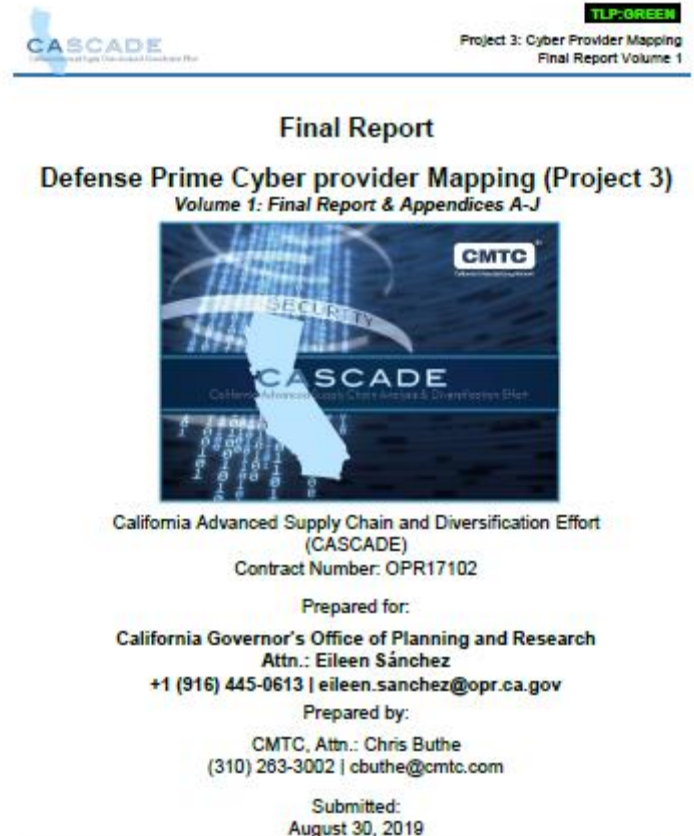
STRENGTHENING ALLIANCES AND BUILDING NEW PARTNERSHIPS

D

Cyber Provider Mapping

Project Summary:

- Examine the Cyber provider marketplace, and their ability to supply critical cyber products and services, in relation to U.S. Department of Defense (DoD) small and medium-size suppliers who are required to comply with the DFARS clause 252.204-7012.

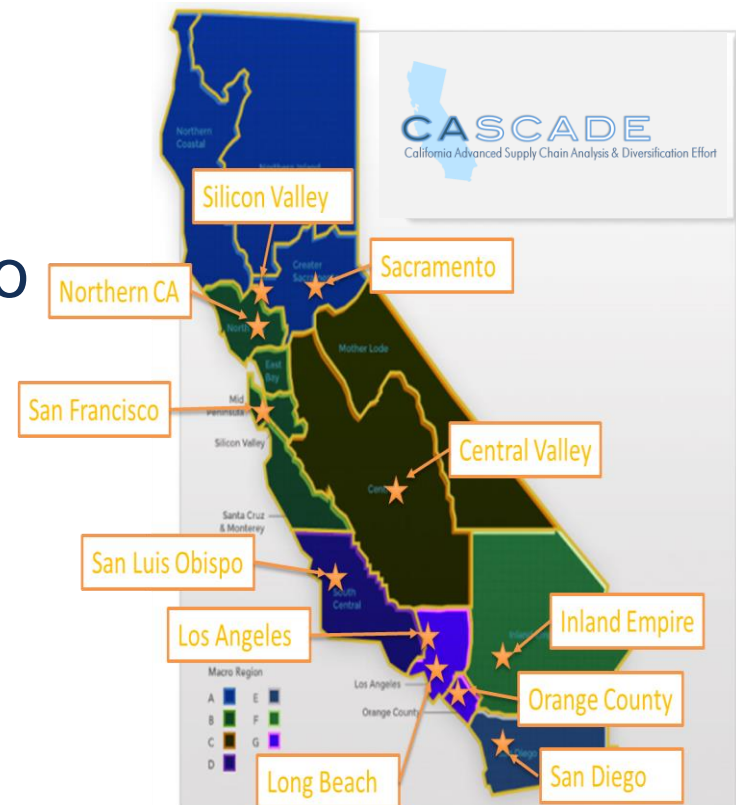


This study was prepared under contract with the California Governor's Office of Planning and Research with financial support from the U.S. Department of Defense, Office of Economic Adjustment. The content reflects the views of CMTC and does not necessarily reflect the views of the U.S. Department of Defense, Office of Economic Adjustment, or the California Governor's Office of Planning and Research.

Regional Resilience Workshops & Resource Fairs

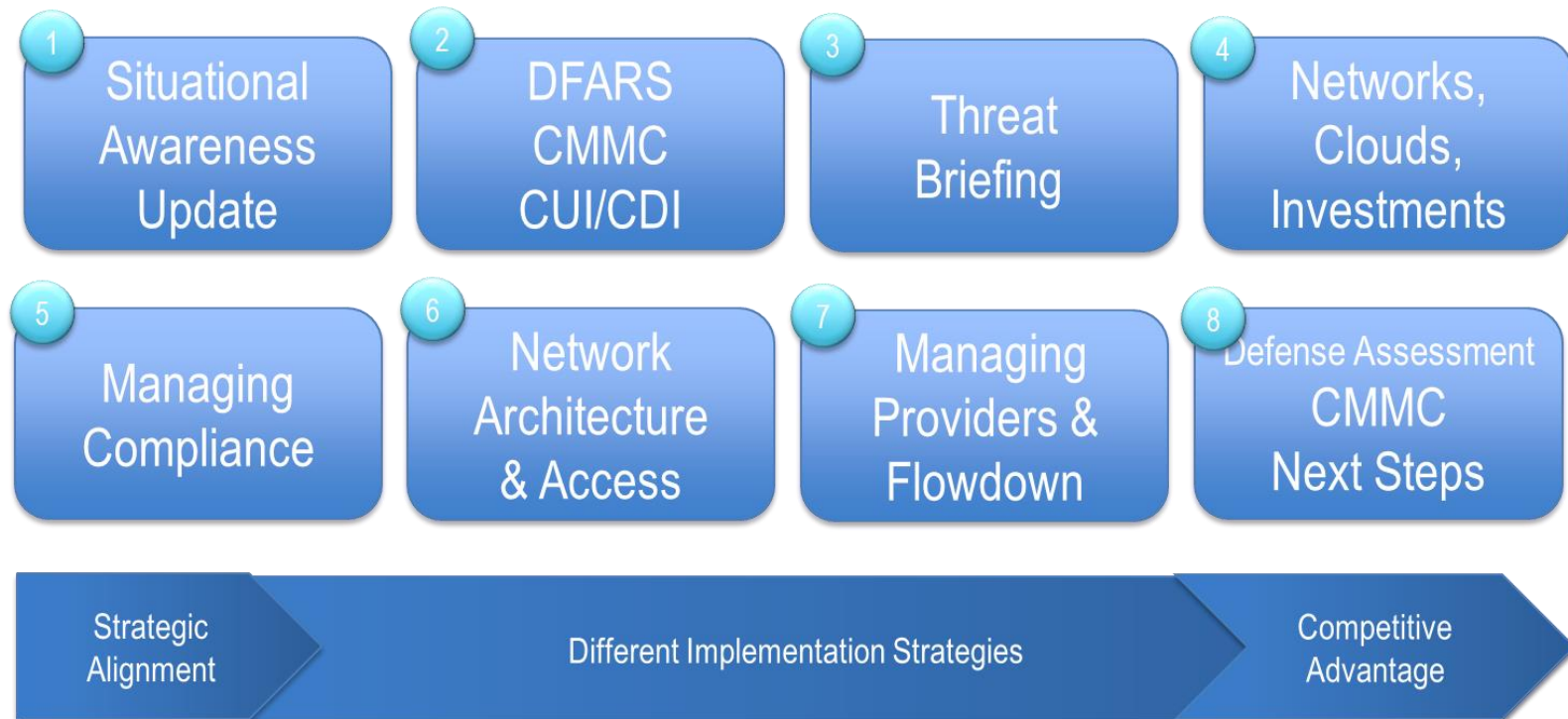
Project summary:

- Workshops in various CA economic regions tailored to respective ecosystem in order to foster supply chain resiliency and focus on industry verticals with ties to defense spending.
- Workshops include tailored agendas and regional partners.



Cybersecurity Bootcamp Format

- Learning modules continuously evolving based on DoD directives



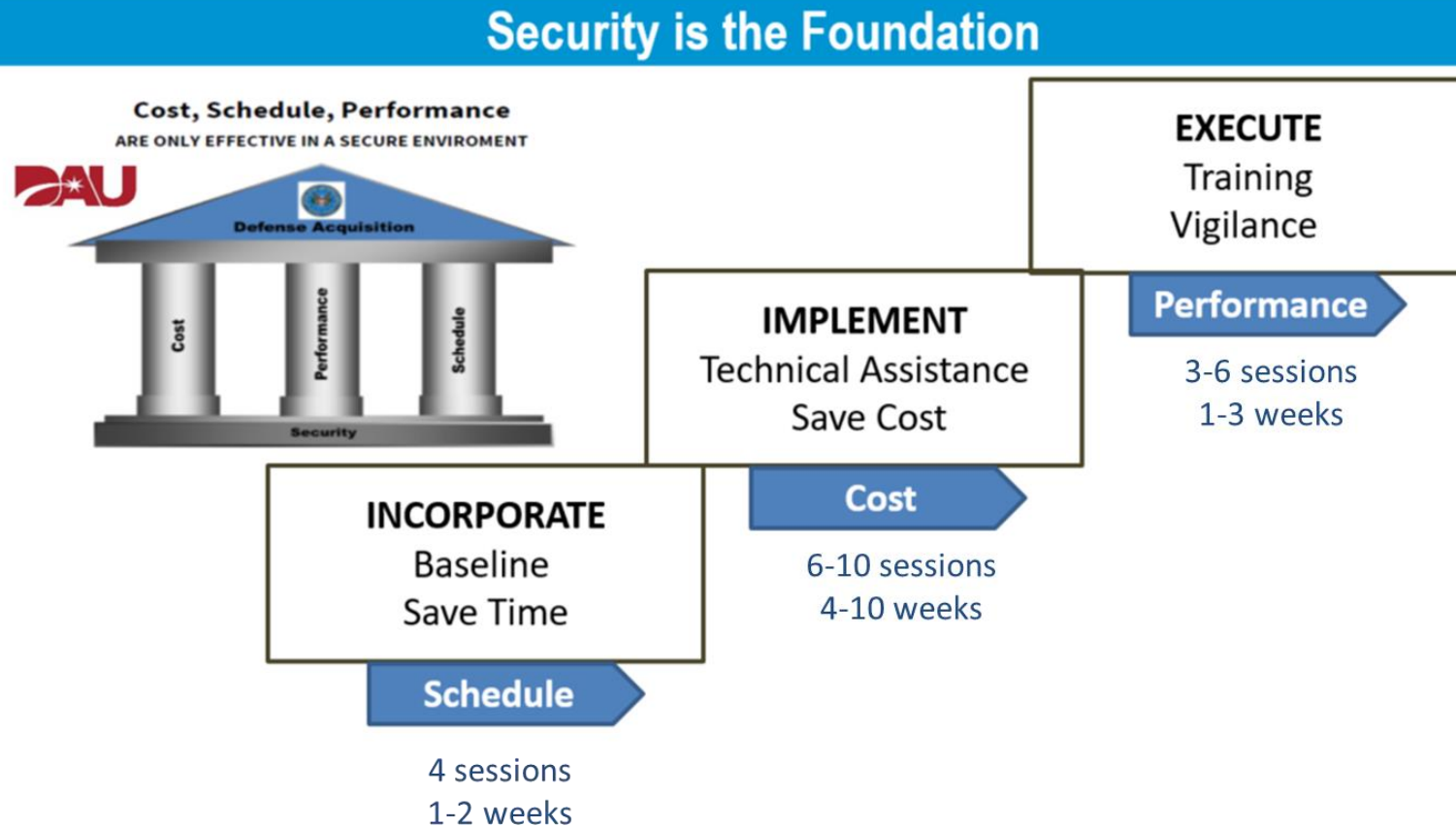
Participating defense suppliers receive:

One (1) full day training workshop – live, at the boot camp

Four (4) one (1) hour follow-up sessions once per month, via phone/web

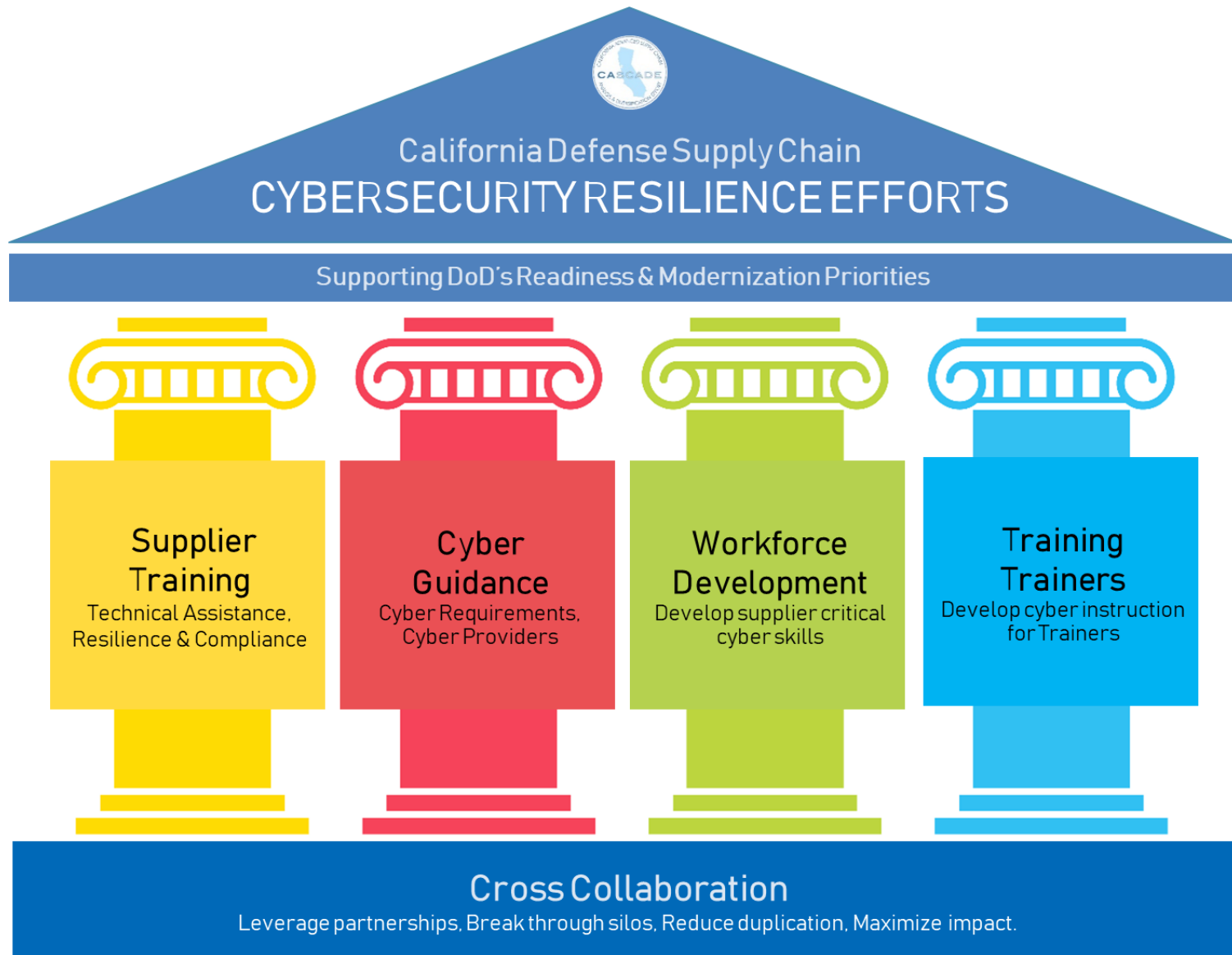
Cybersecurity Assessments

- Compliance and resilience training



CASCADE II - Projects by Deliverable Category





THANK YOU!

- Questions?

Cybersecurity Lessons from Effective Programs



CASCADE
California Advanced Supply Chain Analysis & Diversification Effort



Wrap Up and Closing Thoughts

Mike Gilroy

- Program Director, Industry Resilience
- US Department of Defense/
Office of Economic Adjustment
- Michael.P.Gilroy3.civ@mail.mil

