CREC CENTER FOR REGIONAL ECONOMIC COMPETITIVENESS

Cybersecurity Webinar Series

Presented by OEA and CREC

WELCOME

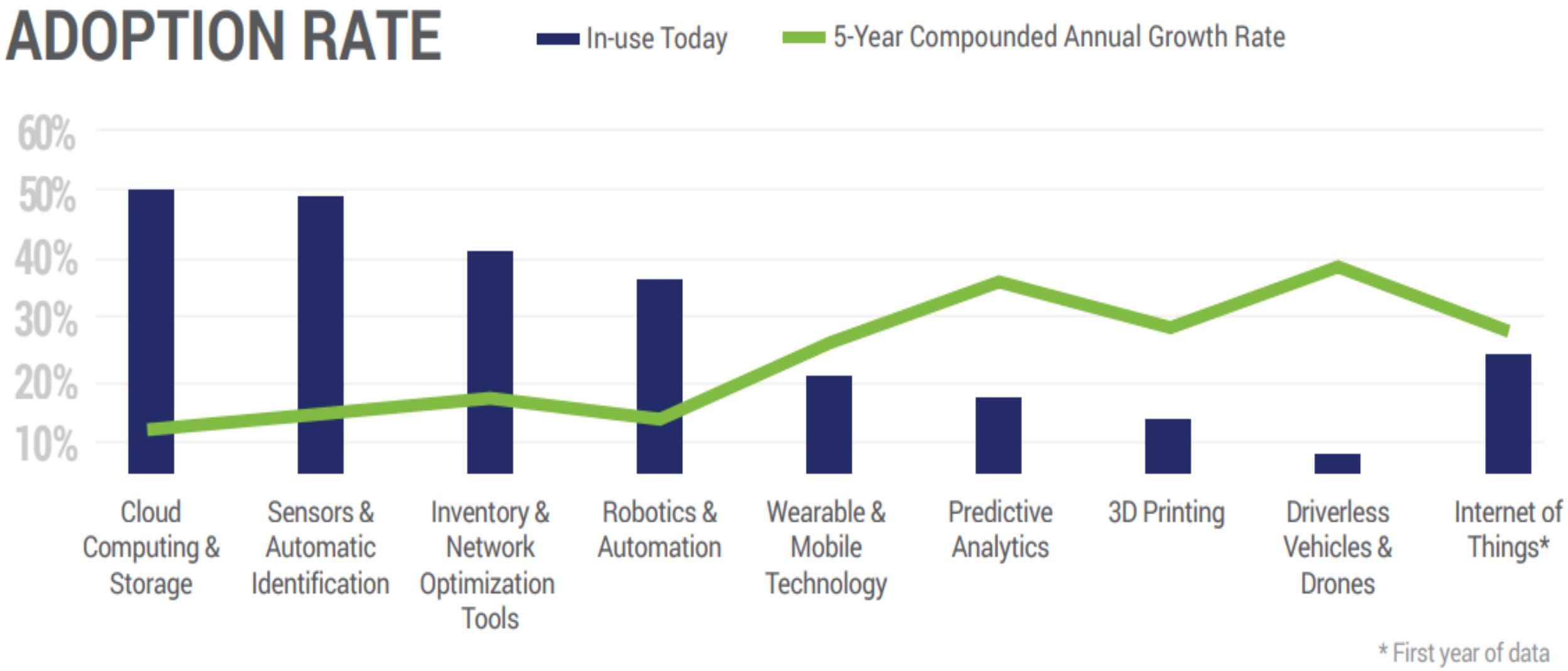
The LATEST on CYBER and the Defense Industry: Collaborating with the Manufacturing Extension Partnership National Network to Reach the Defense Supply Chain

Session Takeaways

- **Speed/Pace** of technological change
- **How** our **National Security** is being affected
- **Effects** of security on business
- **NIST MEP** role – including DoD Project
- **What's** coming next?


MANUFACTURING
AT THE SPEED OF CHANGE


Order Pick Time
01:14:38
Order Pick Time
00:05:15
Order Pick Time
002:09:27
Order Pick Time
15:14:03



2018 Deloitte MHI
Annual Industry Report

MEP National Network

TOP CHALLENGES

Hiring and Retaining a Skilled Workforce

Customer Demand for Faster Response Times

Customer Demand for Lower Delivered Costs

2017 Deloitte MHI Annual Industry Report

MICHIGAN MANUFACTURING TECHNOLOGY CENTER

MANUFACTURE SMARTER

MEP National Network

BARRIERS TO IOT ADOPTION

56%

Cyber Security

45%

Lack of talent to utilize technology effectively.

44%

Lack of a clear business case to justify investment

2018 Deloitte MHI
Annual Industry Report

MICHIGAN MANUFACTURING TECHNOLOGY CENTER

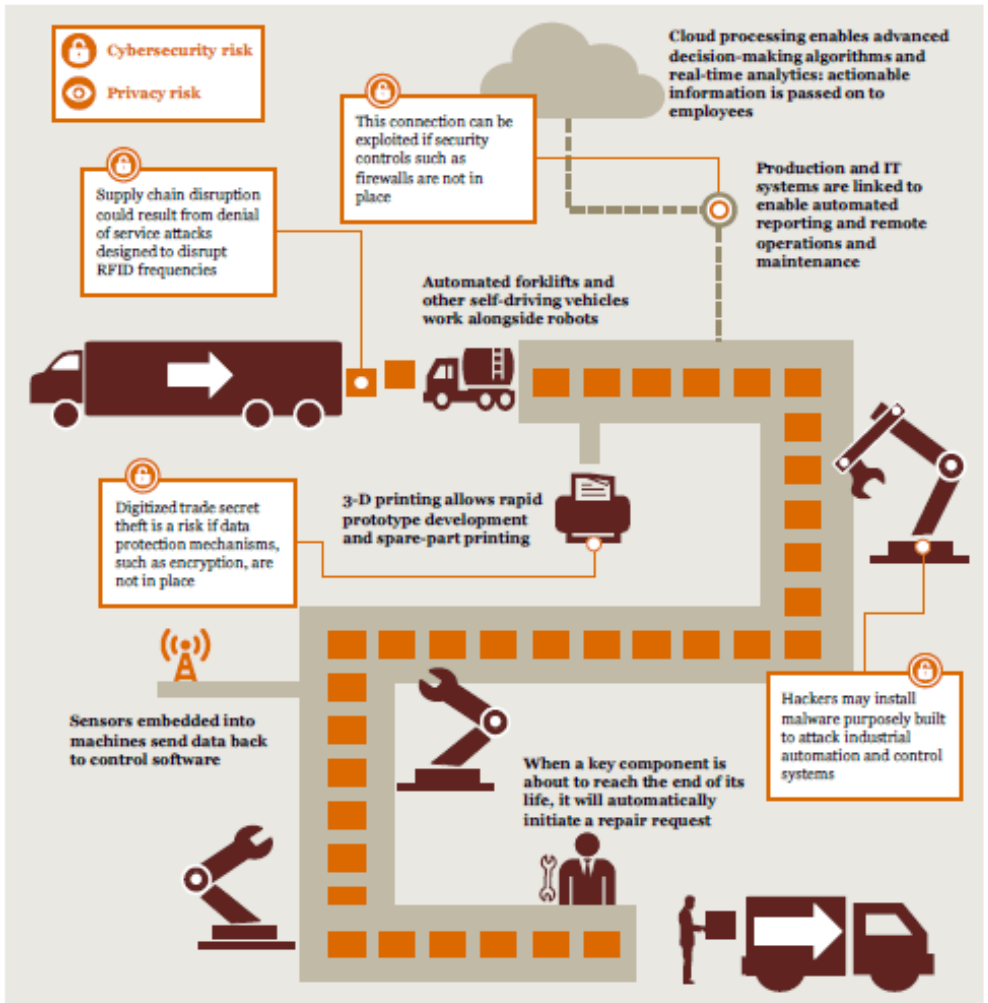
MANUFACTURE SMARTER

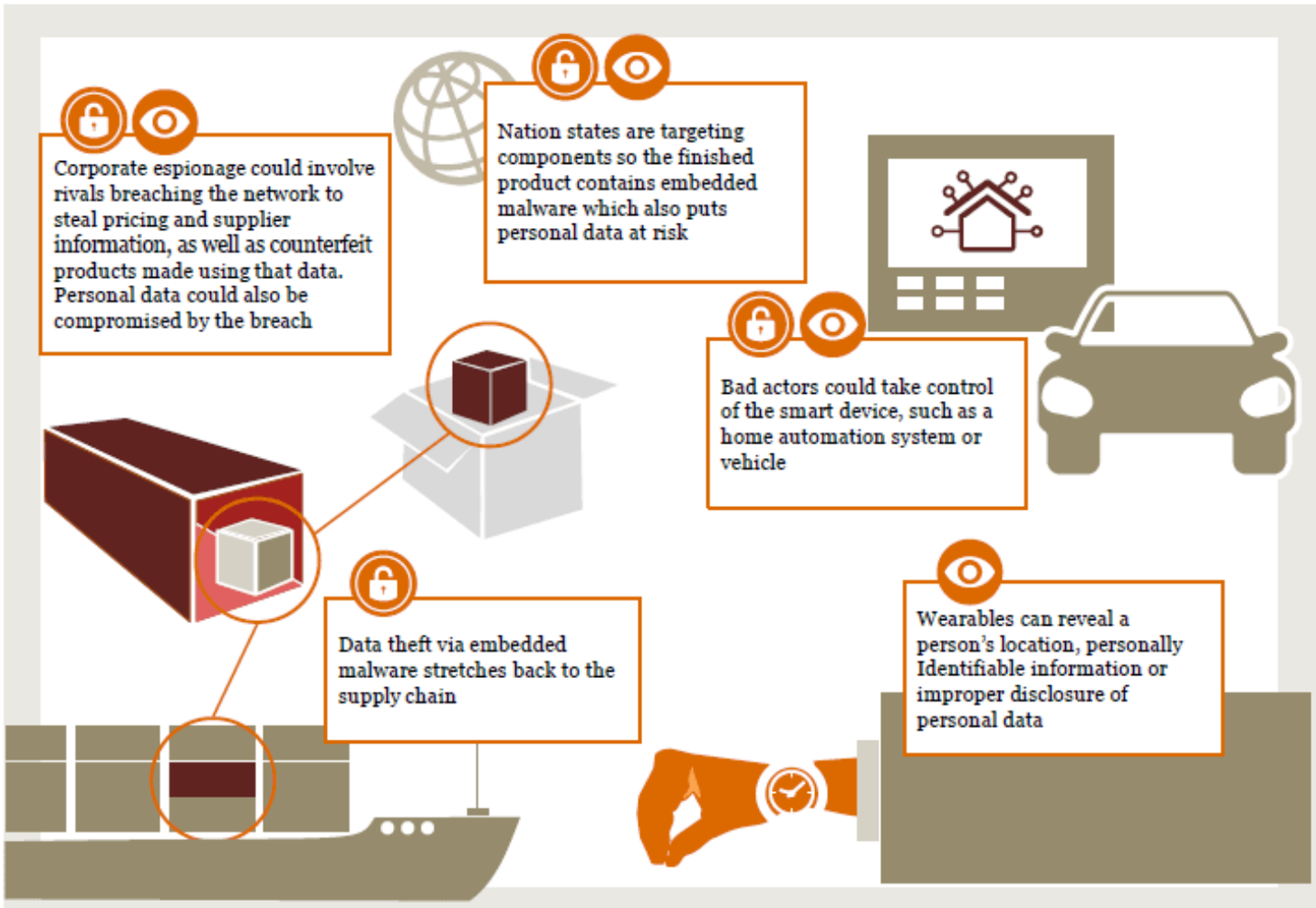
Our appetite for *advanced technology* is rapidly exceeding our ability to protect it.

Complexity

Multitude of applications, dependencies, and connection points are required to fulfill business needs

Cybersecurity risks in action for the manufacturing sector





Cybersecurity: Is it real?

1. There is a hacker attack every **39 seconds**, affecting one in three Americans each year.
2. **43 percent** of cyber attacks target small business
3. **64%** of companies have experience web-based attacks
4. The average cost of a data breach in 2020 will exceed **$150M** as more business infrastructure gets connected
5. Since 2013 there are **3,809,448 records stolen** from breaches every day; **158,727** per hour; **2,645** per minute; and **44** every second

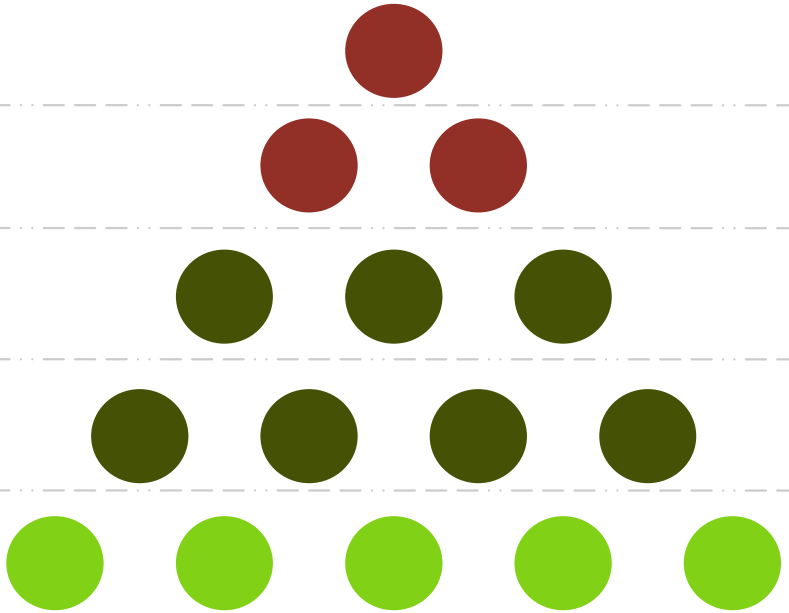
The Burning Platform

NATIONAL SECURITY
U.S. COMPETITIVE TECHNOLOGICAL ADVANTAGE

The FBI estimates the negative U.S financial impact of cybersecurity has already topped ***$1 Trillion*** *during 2019*

CYBER RISK IN THE SUPPLY CHAIN

> “Encourage industry cyber capability and resilience to those areas of the industry most vulnerable … namely the lower tier small and speciality suppliers both direct & indirect.”



	Capability	Exposure
OEM	HIGH	LOW
TIER1	HIGH	LOW
TIER2	MEDIUM	MEDIUM
TIER3	LOW	HIGH
TIER4	LOW	HIGH

There are roughly **370,000** defense contractors in the U.S.

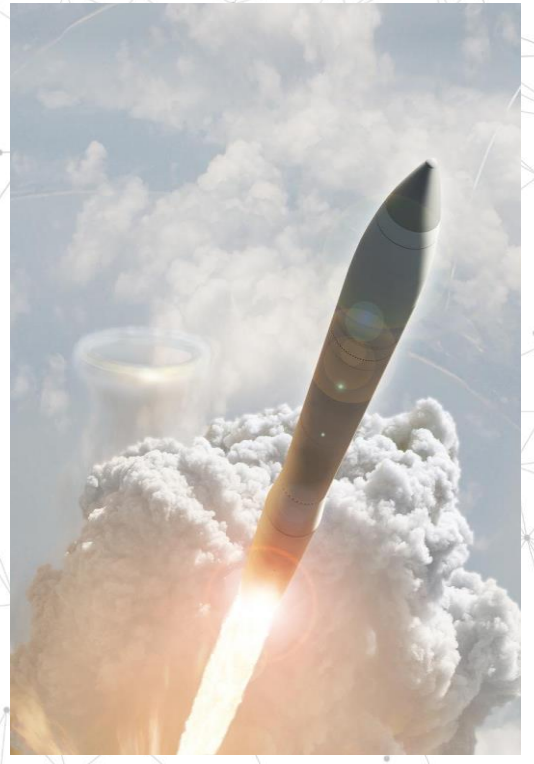
Over **90%** have fewer than **500 employees**

Source: U.S. Census Bureau









MEP National Network™

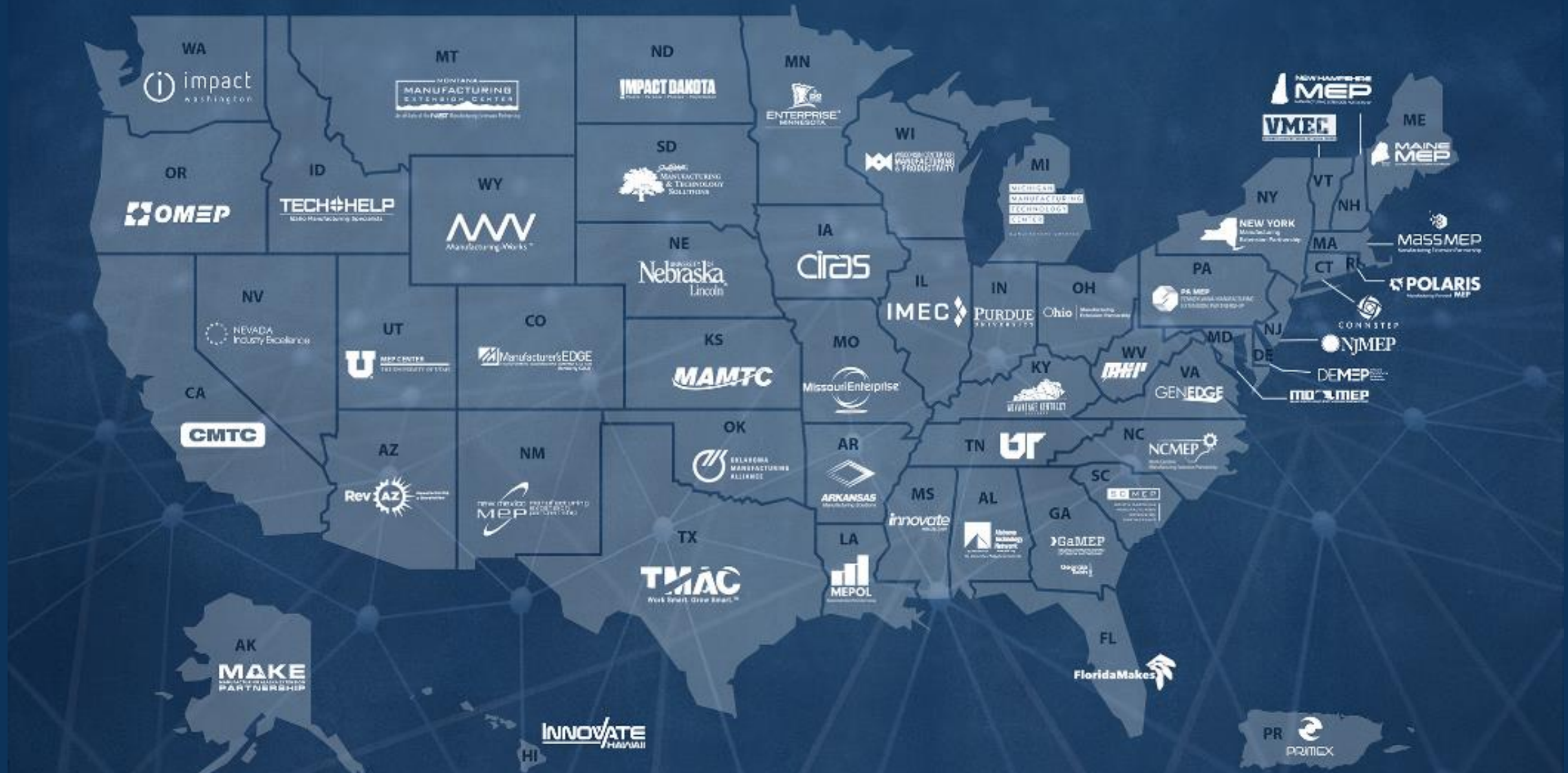
MEP National Network

The Go-to Experts for Advancing U.S. Manufacturing

MEP is **THE** Connection to the U.S. Manufacturing Sector!

MEP National Network™

The Go-To Experts for Advancing U.S. Manufacturing




THE GO-TO EXPERTS FOR ADVANCING U.S. MANUFACTURING
NATIONAL NETWORK
One Center in Every State and Puerto Rico
Over 1,300 Manufacturing Experts
Over 400 Service Locations
Nearly 2,100 Service Providers & Partners
Interacted with 26,313 Manufacturers

Cybersecurity

Notice of Funding Opportunity

Cybersecurity for Defense Manufacturing

MEP Cybersecurity Practice

- Currently, **44 Centers** have an established practice
- Conducted over **1,000 awareness events** nationally
- **Hundreds** of **technical assistance** projects with SMMs
- At least **12 Centers** partnering with **OEA** on projects
- Strong working relationships with **OSD, DAU, OEA, DHS**, etc.

DoD Funding Opportunity

- Demonstrate the **Power** of the **National Network**
- Bring **heightened awareness** throughout the DoD supply chain
  - ✓ *Will touch over **1,000** manufacturers*
- Provide **technical assistance** for manufacturers nationally
- Work with NIST Labs on an effective “How-to” Guide
  - ✓ ***NISTR 8183 -** Manufacturing Profile*
  - ✓ *Operating Technology environment*

Project Priorities – *"Go To MEP Network"*

- National program

  ✓***Majority*** *of MEP Centers are fully engaged, plus many partners*

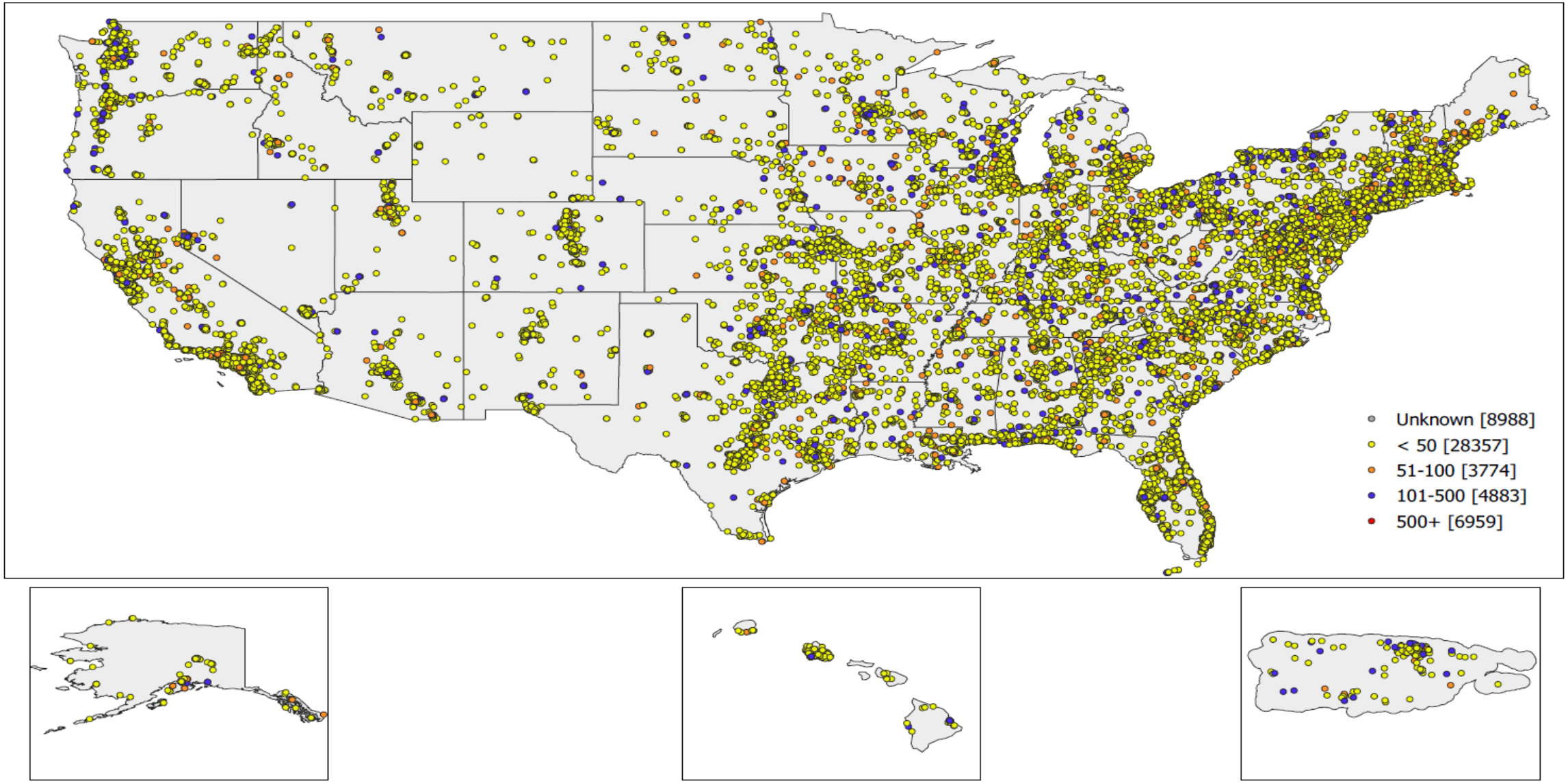
- **3 Tasks** *(Education, Tech Assistance, Use Cases)*
- Educate the Supply Chain to **TAKE ACTION**
- Assist DoD contractors in **resiliency** and **self-attestation**

  ✓*Reasonable and cost-effective approaches*

Task 1 (Education Events)

- Create awareness/education for at least **1,000** companies
  - ✓ ***23*** *In-person events*
  - ✓ ***5*** *recorded webinars*
- No less than **50** companies per event
- Completion date **December 31, 2020**

2018 FY Prime Contractors



Awareness/Education Event Locations

Plymouth, MI	MW	Nov. 22nd
Long Island, NY	NE	Dec. 5th
Providence, RI	NE	Dec. 17th
Orlando, Fla	SE	Jan. 30th
Arlington, Tx	SW	Feb. 11th
Beaumont, Tx	SE	Mar. 10th
Cincinnati, OH	MW	Mar. 10th
Linthicum Heights, MD	East	Mar. 24th
Nashville, TN	SE	Apr. 9th
Pittsburgh, PA	MW	Apr. 16th
Mt. Laurel, NJ	East	Apr 30th
San Diego	W	May 6th

Charleston, SC	SE	May 20th
Akron, OH	MW	June 9th
Wichita, KS	MW	June 17th
St. Louis, MO	MW	July 15th
Seattle, WA	West	Aug. 9th
Denver, CO	Mountain	Aug. 20th
Chicago, IL	MW	Sept. 20th
Newport News, VA.	East	TBD
Huntsville, AL	SE	TBD
FL Panhandle	SE	TBD
Northern CA	West	TBD

Educational Event Outline (6 hrs.)

- **Cyber Resilience** (Risk Management / System Design)
  - What is cyber resilience?
  - Steps involved in preparing and creating an RMS
  - Documents that should be produced / outcome
  - Importance of Policy/Procedures
  - Importance of Testing and Validation

- **Requirements to fulfill DFARS obligations**
  - NIST 800-171 and how it applies to DFARS and an RMP
  - What is “cloud computing” and understanding the requirements as it pertains to DFARS
  - Cyber incident reporting and the requirements.
  - Supply Chain Flow down

- **The future of Cyber requirements in the DoD**

Task 2 (Technical Assistance)

- Conduct at minimum **10** Technical Assistance Projects
- To be completed by **December 31, 2020**

Task 2 (Technical Assistance)

1. Must be a Small to Mid-Size Manufacturer
2. Creates/receives CUI
3. Part of the Critical Manufacturing Infrastructure
4. Committed to project and to maintaining cyber resiliency

Task 2 (Technical Assistance)

- **Cyber Resilience/Risk Management** - Analysis and Development Assessment against **800-171 rev 1**.
- *Project Plan* development (including appropriate areas from 800-171b and CMMC)
- Required documentation/practices for DFARS (System Security Plan, Plan of Action with Milestones, Incident Response Plan)
- Includes 1yr of **vulnerability scans** and **Risk Management / Compliancy** progress tracking utility

Task 3 (Use Cases - OT)

- Compete Use Cases based on Manufacturing Profile
  - ✓***NISTR 8183***
  - ✓*Focus – **shop floor vulnerabilities** (Operating Technology)*
- Test case the Profile in full implementation
- NIST Labs is the customer

Strength of the Community

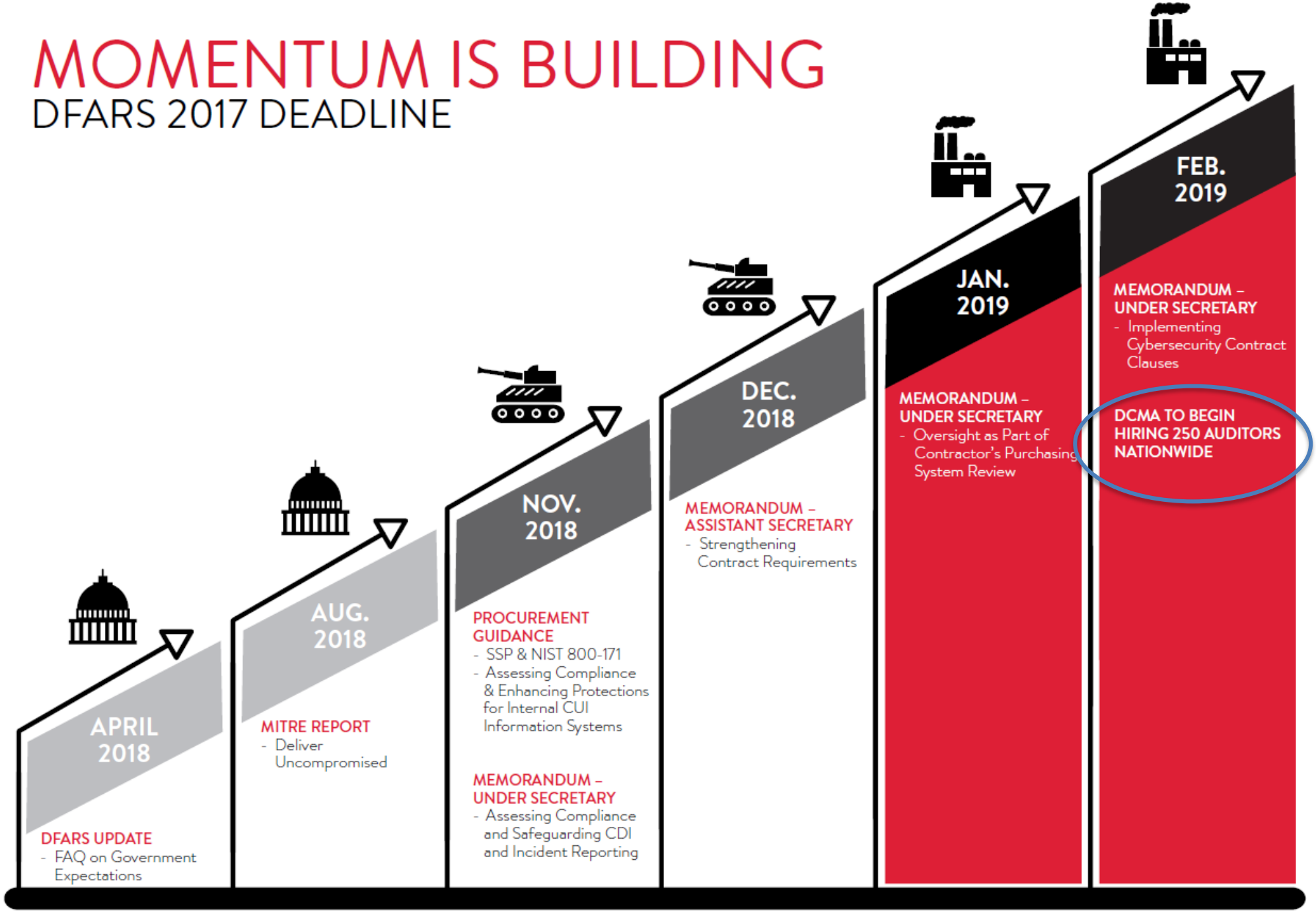
Your Involvement and partnership!

- ✓ *Reinforcing importance – National Security and business viability*
- ✓ *Creating Awareness*
- ✓ *Participating in Educational Events*
- ✓ *Explore partnerships as resources for technical expertise*

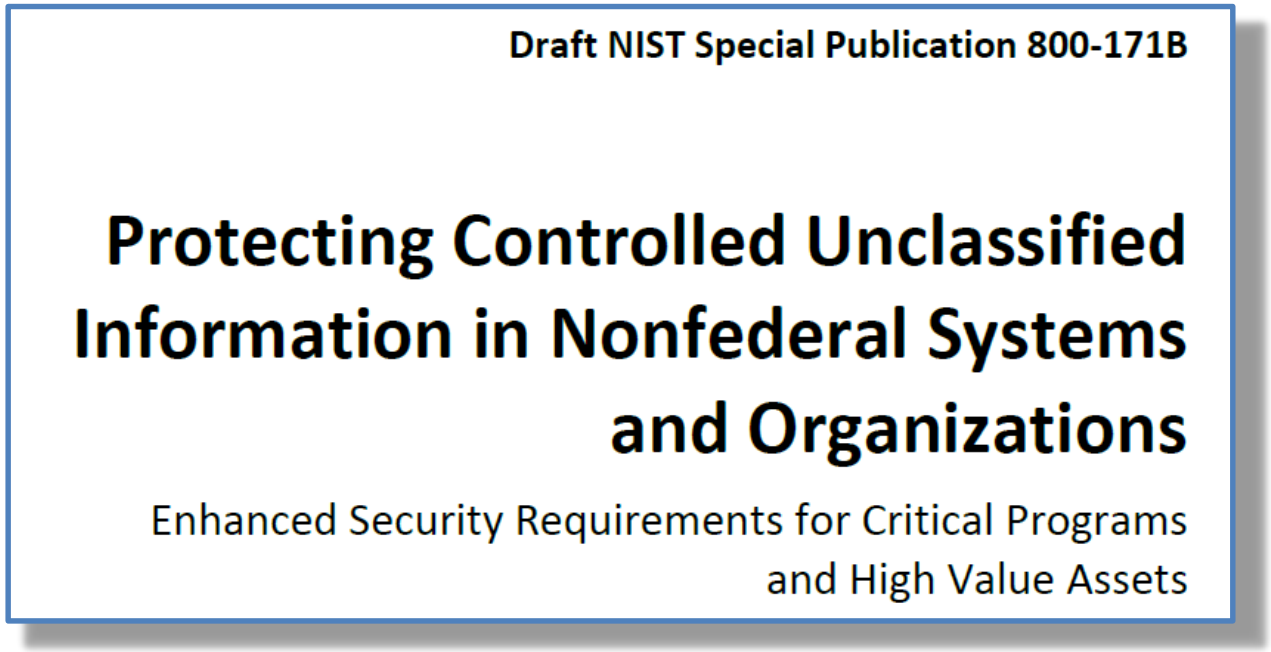

What's Next?

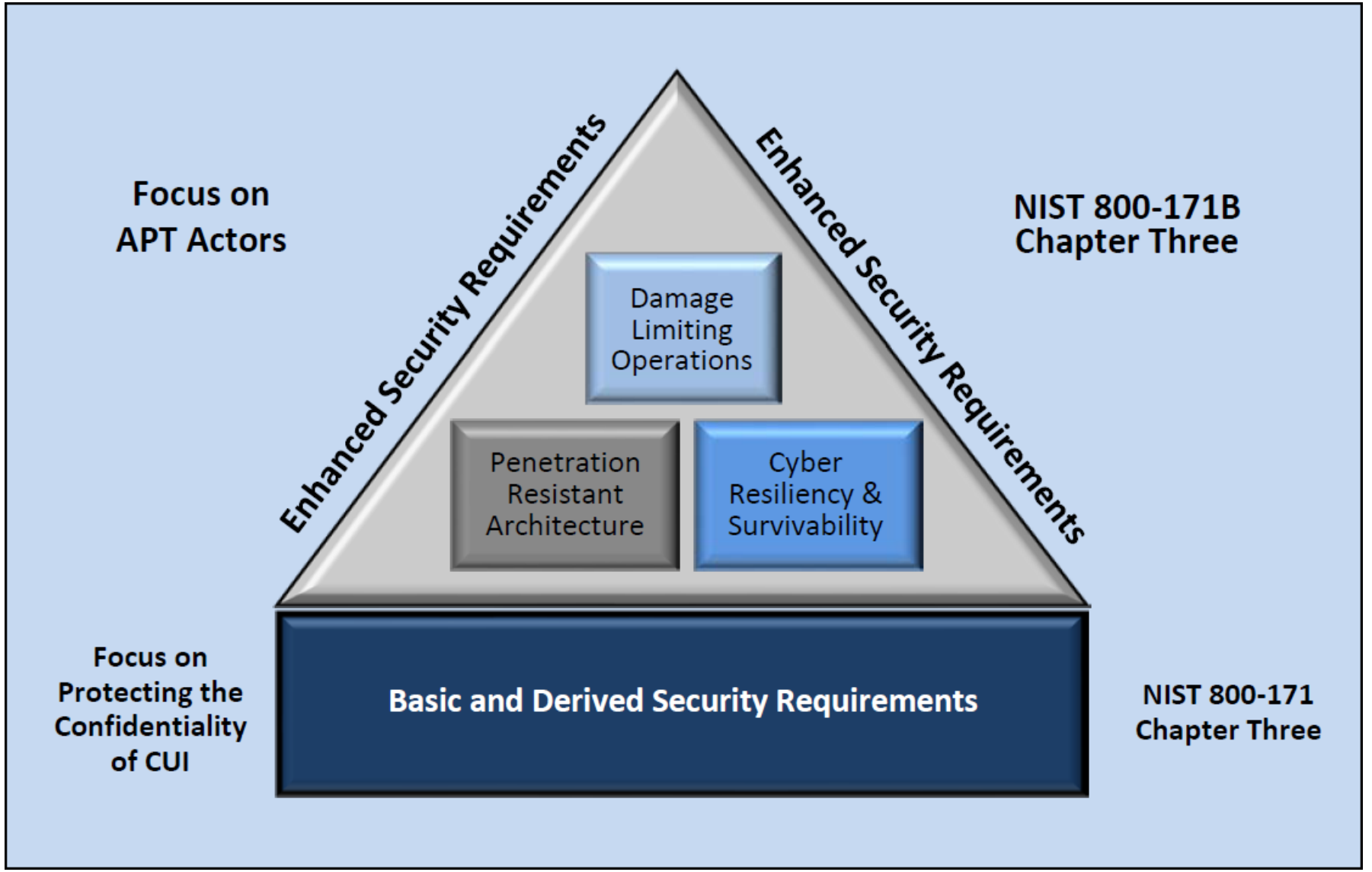
MOMENTUM IS BUILDING

DFARS 2017 DEADLINE



NIST SP 800-171B – *Enhanced Security Requirements for Critical Programs and High Value Assets*



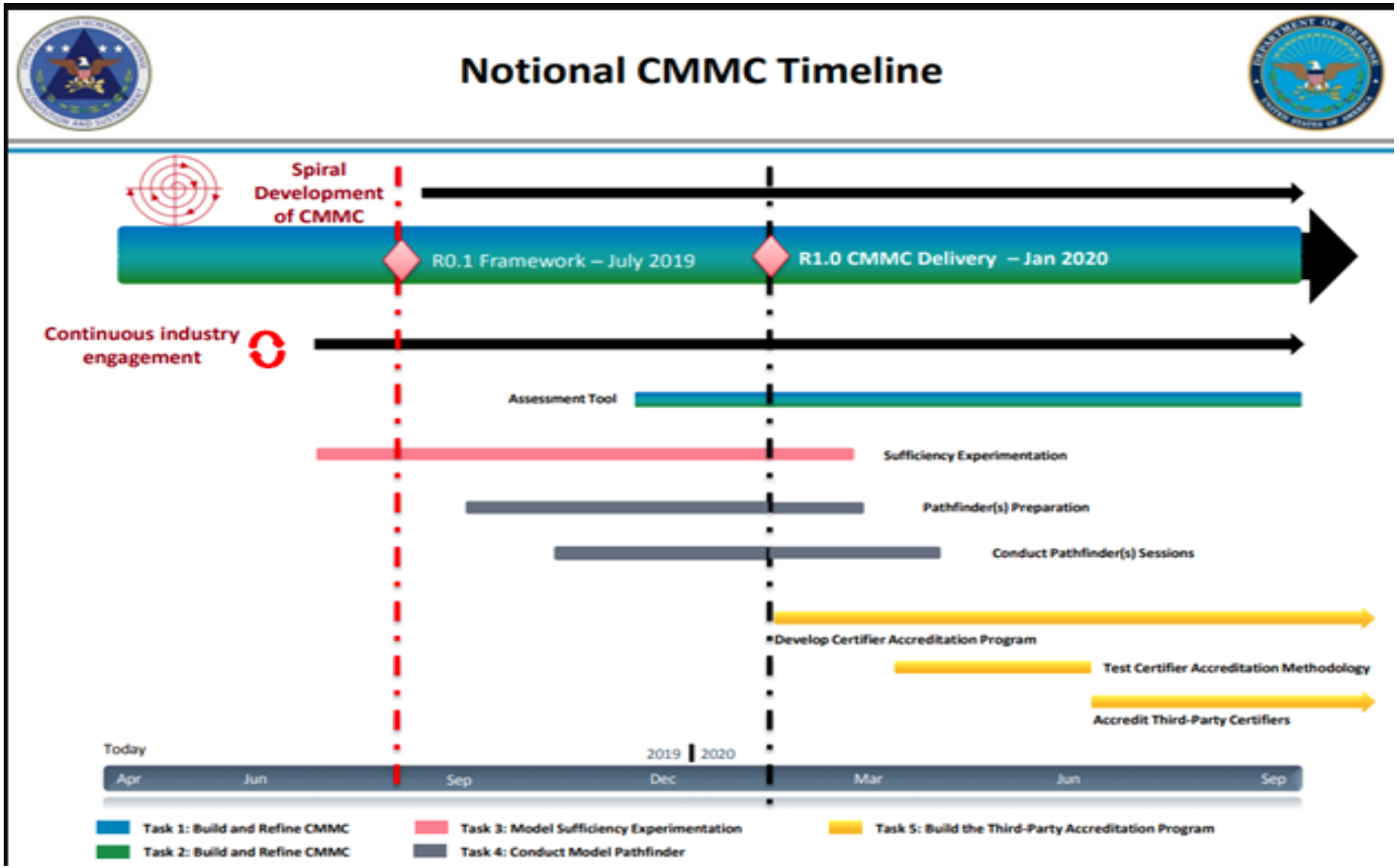

Focus on APT Actors
Enhanced Security Requirements
Enhanced Security Requirements
NIST 800-171B Chapter Three
Damage Limiting Operations
Penetration Resistant Architecture
Cyber Resiliency & Survivability
Focus on Protecting the Confidentiality of CUI
Basic and Derived Security Requirements
NIST 800-171 Chapter Three


CMMC
Cybersecurity Maturity Model Certification
THE NEW CYBERSECURITY STANDARD

How Does CMMC Differ from DFARS 252.204-7012?

DFARS 252.204-7012	CMMC
Applies only to contractors who handle CDI	Applies to all contractors conducting business with the DoD
Single Level (Compliance or Noncompliance)	Multiple Levels of “maturity” from Basic Cyber protection to fully mature cybersecurity practices
Requires Self Attestation to Compliancy	Requires Certification from Third Party entity

	Level 1	Level 2	Level 3	Level 4	Level 5
Technical Practices	Demonstrate basic cyber hygiene, as achieved by the Federal Acquisition Regulation (FAR)	Demonstrate intermediate cyber hygiene	Demonstrate good cyber hygiene and effective NIST SP 800-171 Rev 1 security requirements	Demonstrate a substantial and proactive cybersecurity program	Demonstrate a proven ability to optimize capabilities in an effort to repel advanced persistent threats
Process Maturity	No process maturity	Standard operating procedures, policies, and plans are established for all practices	Activities are reviewed for adherence to policy and procedures and adequately resourced	Activities are reviewed effectiveness and management is informed of any issues	Activities are standardized across all applicable organizational units and identified improvements are shared


Notional CMMC Timeline
Spiral Development of CMMC
R0.1 Framework – July 2019
R1.0 CMMC Delivery – Jan 2020
Continuous industry engagement
Assessment Tool
Sufficiency Experimentation
Pathfinder(s) Preparation
Conduct Pathfinder(s) Sessions
Develop Certifier Accreditation Program
Test Certifier Accreditation Methodology
Accredit Third-Party Certifiers
Today
2019
2020
Apr
Jun
Sep
Dec
Mar
Jun
Sep
Task 1: Build and Refine CMMC
Task 2: Build and Refine CMMC
Task 3: Model Sufficiency Experimentation
Task 4: Conduct Model Pathfinder
Task 5: Build the Third-Party Accreditation Program

AUTOMOTIVE OEM GUIDANCE

Personally Identifiable Information (pii)

- WHAT IS PII?
  - PII is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.

What should I be doing?

MEP National Network™

- Focus on **current contractual requirements** and establishing **cyber resilience**.
  - ✓***DFARS 252.204-7012*** *is* ***"Current"*** *requirements and past compliancy deadline*
  - ✓***Review Plan of Actions with Milestones*** *(PoAM) and address any outstanding items*

- Threats are constantly changing. Requirements and "Resiliency" are adapted to these threats.

Remember…

- Keep solutions **Practical**
- Mostly about **Policies & Practices**
- Create **Behavior** change

Summary

Protecting your Business **IS NOT** Optional

Continuously monitor / remove **Vulnerabilities**

Understand procedures are **intertwined**


QUESTIONS?

Elliot Forsyth
eforsyth@the-center.com
734-451-4212

Other Resources

Under Secretary Lord Press Briefing – 12.10.2019
https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/2037206/under-secretary-of-defense-for-acquisition-sustainment-ellen-lord-press-briefin/

DCMA Audit Process – 11.14.2019
https://www.acq.osd.mil/dpap/pdi/cyber/docs/14%20Nov%202019%20USD(A&S)%20Memo%20Assessing%20Contractor%20Implementation%20of%20Cybersecurity%20Requirements.pdf

Other Resources

Memo Assessing Contractor Implementation of Cyber Requirements – 11.14.2019

https://www.acq.osd.mil/dpap/pdi/cyber/docs/14%20Nov%202019%20USD(A&S)%20Memo%20Assessing%20Contractor%20Implementation%20of%20Cybersecurity%20Requirements.pdf

NIST 800-171 DoD Assessment Methodology V1– 11.7.2019

https://nam01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.acq.osd.mil%2Fdpap%2Fpdi%2Fcyber%2Fdocs%2FNIST%2520SP%2520800-171%2520DoD%2520Assessment%2520Methodology.pdf&data=02%7C01%7Ceforsyth%40the-center.org%7C5db529865a7f4d401ec908d76ee55dfa%7C4163507b51d847738856637ff1a52656%7C1%7C1%7C637099803724841920&sdata=aUAAps2dVwkLXpRCMe58kqrQdcLXcJ724nTRvzmzAo4%3D&reserved=0

Previous Cybersecurity Webinars

New NDIA Report Explores Cyber Threats and Responses in the Defense Industry – November 21st 2019

CREC hosted a webinar to discuss the National Defense Industry Association's recent paper, "Beyond Obfuscation: The Defense Industry's Position within Federal Cybersecurity Policy," presented by Corbin Evans from NDIA.

http://creconline.org/project-update/new-ndia-report-explores-cyber-threats-and-responses-in-the-defense-industry/

The Latest on CYBER and the Defense Industry: Collaborating with the MEP National Network to Reach the Defense Supply Chain – December 17th 2019

CREC hosted a webinar on the NIST MEP National Network effort to provide cybersecurity awareness training and implementation services to manufacturers, presented by Elliot Forsyth from the Michigan Manufacturing Technology Center.

All previous programming is available on the CREC website and distributed via the Industry Resilience Bulletin. Please contact Lee Winkler (lwinkler@crec.net , 703-522-4980, ext. 1029) for assistance in accessing any previous webinars. All slides will be posted on the CREC website.

Future OEA Related Programming

Supply Chain Webinar – December 19th 2019 at 11:30 am EST

Join CREC and Entreworks Consulting for a webinar reviewing efforts funded by OEA to strengthen supply chains and the defense industrial base in your region.

https://register.gotowebinar.com/register/9420861552774197 88

C2ER California Cybersecurity Webinar – January 14th 2020 at 2 pm EST

Join a free webinar on a California survey of the state's cybersecurity workforce, focusing on middle-skill IT workers, including findings and implications. There is a listed registration fee for non-members that should be waived.

https://www.c2er.org/events/webinars.asp

Cyber Collaboration Center Webinar – January 22nd at 4 pm EST

Join the Cyber Collaboration Center in reviewing the DoD Assessment Methodology v1.0 and its relation to CMMC and DFARS cybersecurity. Please check https://www.cybercollaborationcenter.org/ for the registration link.

CMMC Release Webinar – Late January/Early February 2020 – TBD

Join CREC to discuss the release of CMMC, its impact on the defense industrial base, and how OEA grantees and partners can respond. Programming still TBD. Please check the IR Bulletin for details.