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

- Cloud Computing & Storage: In-use Today 50%, 5-Year CAGR 40%
- Sensors & Automatic Identification: In-use Today 45%, 5-Year CAGR 30%
- Inventory & Network Optimization Tools: In-use Today 40%, 5-Year CAGR 20%
- Robotics & Automation: In-use Today 30%, 5-Year CAGR 10%
- Wearable & Mobile Technology: In-use Today 20%, 5-Year CAGR 5%
- Predictive Analytics: In-use Today 10%, 5-Year CAGR 10%
- 3D Printing: In-use Today 5%, 5-Year CAGR 2%
- Driverless Vehicles & Drones: In-use Today 2%, 5-Year CAGR 1%
- Internet of Things*: In-use Today 1%, 5-Year CAGR 1%

* First year of data

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

- Hiring and Retaining a Skilled Workforce: 63%
- Customer Demand for Faster Response Times: 55%
- Customer Demand for Lower Delivered Costs: 53%
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
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 risk**
- **Privacy risk**
- **Supply chain disruption** could result from denial of service attacks designed to disrupt IoT frequencies.
- **Cloud processing** enables advanced decision-making algorithms and real-time analytics actionable information is passed on to employees.
- **Automated forklifts** and other self-driving vehicles work alongside robots.
- **3D printing** allows rapid prototyping development and spare-part printing.
- **Data theft** via embedded malware stretches back to the supply chain.
- **Wearables** can reveal a person's location, personally identifiable information or improper disclosure of personal data.
- **Corporate espionage** could involve rivals breaching the network to steal pricing and supplier information, as well as counterfeit products made using that data. Personal data could also be compromised by the breach.
- **Nation states** are targeting components so the finished product contains embedded malware which also puts personal data at risk.
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 FBI estimates the negative U.S. financial impact of cybersecurity has already topped $1 Trillion during 2019.
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.

**CYBER RISK IN THE SUPPLY CHAIN**

<table>
<thead>
<tr>
<th>Tier</th>
<th>Capability</th>
<th>Exposure</th>
</tr>
</thead>
<tbody>
<tr>
<td>OEM</td>
<td>HIGH</td>
<td>LOW</td>
</tr>
<tr>
<td>TIER1</td>
<td>HIGH</td>
<td>LOW</td>
</tr>
<tr>
<td>TIER2</td>
<td>MEDIUM</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>TIER3</td>
<td>LOW</td>
<td>HIGH</td>
</tr>
<tr>
<td>TIER4</td>
<td>LOW</td>
<td>HIGH</td>
</tr>
</tbody>
</table>
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
The Go-to Experts for Advancing U.S. Manufacturing
MEP is **THE** Connection to the U.S. Manufacturing Sector!
The Go-To Experts for Advancing U.S. Manufacturing
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
The Go-to Experts for Advancing U.S. 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

- Unknown [8988]
- < 50 [28357]
- 51-100 [3774]
- 101-500 [4883]
- 500+ [5959]
# Awareness/Education Event Locations

<table>
<thead>
<tr>
<th>Location</th>
<th>Region</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plymouth, MI</td>
<td>MW</td>
<td>Nov. 22&lt;sup&gt;nd&lt;/sup&gt;</td>
</tr>
<tr>
<td>Long Island, NY</td>
<td>NE</td>
<td>Dec. 5&lt;sup&gt;th&lt;/sup&gt;</td>
</tr>
<tr>
<td>Providence, RI</td>
<td>NE</td>
<td>Dec. 17&lt;sup&gt;th&lt;/sup&gt;</td>
</tr>
<tr>
<td>Orlando, Fla</td>
<td>SE</td>
<td>Jan. 30&lt;sup&gt;th&lt;/sup&gt;</td>
</tr>
<tr>
<td>Arlington, Tx</td>
<td>SW</td>
<td>Feb. 11&lt;sup&gt;th&lt;/sup&gt;</td>
</tr>
<tr>
<td>Beaumont, Tx</td>
<td>SE</td>
<td>Mar. 10&lt;sup&gt;th&lt;/sup&gt;</td>
</tr>
<tr>
<td>Cincinnati, OH</td>
<td>MW</td>
<td>Mar. 10&lt;sup&gt;th&lt;/sup&gt;</td>
</tr>
<tr>
<td>Linthicum Heights, MD</td>
<td>East</td>
<td>Mar. 24&lt;sup&gt;th&lt;/sup&gt;</td>
</tr>
<tr>
<td>Nashville, TN</td>
<td>SE</td>
<td>Apr. 9&lt;sup&gt;th&lt;/sup&gt;</td>
</tr>
<tr>
<td>Pittsburgh, PA</td>
<td>MW</td>
<td>Apr. 16&lt;sup&gt;th&lt;/sup&gt;</td>
</tr>
<tr>
<td>Mt. Laurel, NJ</td>
<td>East</td>
<td>Apr 30th</td>
</tr>
<tr>
<td>San Diego</td>
<td>W</td>
<td>May 6th</td>
</tr>
<tr>
<td>Charleston, SC</td>
<td>SE</td>
<td>May 20&lt;sup&gt;th&lt;/sup&gt;</td>
</tr>
<tr>
<td>Akron, OH</td>
<td>MW</td>
<td>June 9&lt;sup&gt;th&lt;/sup&gt;</td>
</tr>
<tr>
<td>Wichita, KS</td>
<td>MW</td>
<td>June 17&lt;sup&gt;th&lt;/sup&gt;</td>
</tr>
<tr>
<td>St. Louis, MO</td>
<td>MW</td>
<td>July 15&lt;sup&gt;th&lt;/sup&gt;</td>
</tr>
<tr>
<td>Seattle, WA</td>
<td>West</td>
<td>Aug. 9&lt;sup&gt;th&lt;/sup&gt;</td>
</tr>
<tr>
<td>Denver, CO</td>
<td>Mountain</td>
<td>Aug. 20&lt;sup&gt;th&lt;/sup&gt;</td>
</tr>
<tr>
<td>Chicago, IL</td>
<td>MW</td>
<td>Sept. 20&lt;sup&gt;th&lt;/sup&gt;</td>
</tr>
<tr>
<td>Newport News, VA.</td>
<td>East</td>
<td>TBD</td>
</tr>
<tr>
<td>Huntsville, AL</td>
<td>SE</td>
<td>TBD</td>
</tr>
<tr>
<td>FL Panhandle</td>
<td>SE</td>
<td>TBD</td>
</tr>
<tr>
<td>Northern CA</td>
<td>West</td>
<td>TBD</td>
</tr>
</tbody>
</table>
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
MOMENTUM IS BUILDING
DFARS 2017 DEADLINE

FEB. 2019
MEMORANDUM – UNDER SECRETARY
- Implementing Cybersecurity Contract Clauses

DCMA TO BEGIN HIRING 250 AUDITORS NATIONWIDE

JAN. 2019
MEMORANDUM – UNDER SECRETARY
- Oversight as Part of Contractor’s Purchasing System Review

DEC. 2018
MEMORANDUM – ASSISTANT SECRETARY
- Strengthening Contract Requirements

NOV. 2018
PROCUREMENT GUIDANCE
- SSP & NIST 800-171
- Assessing Compliance & Enhancing Protections for Internal CUI Information Systems

AUG. 2018
MITRE REPORT
- Deliver Uncompromised

APRIL 2018
DFARS UPDATE
- FAQ on Government Expectations

The Go to Experts for Advancing U.S. Manufacturing
NIST SP 800-171B – Enhanced Security Requirements for Critical Programs and High Value Assets
The Go-to Experts for Advancing U.S. Manufacturing

CMMC
Cybersecurity Maturity Model Certification
The New Cybersecurity Standard
## How Does CMMC Differ from DFARS 252.204-7012?

<table>
<thead>
<tr>
<th>DFARS 252.204-7012</th>
<th>CMMC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applies only to contractors who handle CDI</td>
<td>Applies to all contractors conducting business with the DoD</td>
</tr>
<tr>
<td>Single Level (Compliance or Noncompliance)</td>
<td>Multiple Levels of “maturity” from Basic Cyber protection to fully mature cybersecurity practices</td>
</tr>
<tr>
<td>Requires Self Attestation to Compliancy</td>
<td>Requires Certification from Third Party entity</td>
</tr>
</tbody>
</table>
### The Go-to Experts for Advancing U.S. Manufacturing

<table>
<thead>
<tr>
<th>Technical Practices</th>
<th>Level 1</th>
<th>Demonstrate basic cyber hygiene, as achieved by the Federal Acquisition Regulation (FAR)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Level 2</td>
<td>Demonstrate intermediate cyber hygiene</td>
</tr>
<tr>
<td></td>
<td>Level 3</td>
<td>Demonstrate good cyber hygiene and effective NIST SP 800-171 Rev 1 security requirements</td>
</tr>
<tr>
<td></td>
<td>Level 4</td>
<td>Demonstrate a substantial and proactive cybersecurity program</td>
</tr>
<tr>
<td></td>
<td>Level 5</td>
<td>Demonstrate a proven ability to optimize capabilities in an effort to repel advanced persistent threats</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Process Maturity</th>
<th>Level 1</th>
<th>No process maturity</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Level 2</td>
<td>Standard operating procedures, policies, and plans are established for all practices</td>
</tr>
<tr>
<td></td>
<td>Level 3</td>
<td>Activities are reviewed for adherence to policy and procedures and adequately resourced</td>
</tr>
<tr>
<td></td>
<td>Level 4</td>
<td>Activities are reviewed for effectiveness and management is informed of any issues</td>
</tr>
<tr>
<td></td>
<td>Level 5</td>
<td>Activities are standardized across all applicable organizational units and identified improvements are shared</td>
</tr>
</tbody>
</table>
AUTOMOTIVE OEM GUIDANCE

Ford

GM

AIAG

FCA

Honda
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?
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

Other Resources


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%20SP%20800-171%2520DoD%2520Assessment%2520Methodology%2520V1.pdf&data=02%7C01%7Ceforsyth%40the-center.org%7C5db529865a7f4d401ec908d76ee55dfa%7C4163507b51d847738856637ff1a52656%7C1%7C1%7C637099803724841920&ssdata=aUAAps2dVwkLXpRCMe58kqrQdcLXcJ724nTRvmzAo4%3D&reserved=0
Previous Cybersecurity Webinars

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.

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

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/942086155277419788

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.