

National Cybersecurity Center of Excellence

Manufacturing COI call

January 23, 2020

> Agenda

- Welcome
 - Engagement Model
- Project Status Update
 - Timeline
 - Quick project overview
 - Call for collaborators
- Guest Speaker: David Stieren
- Q&A



> Engagement & Business Model

DEFINE



ASSEMBLE



BUILD



ADVOCATE



OUTCOME:

Define a scope of work with industry to solve a pressing cybersecurity challenge



OUTCOME:

Assemble teams of industry orgs, govt agencies, and academic institutions to address all aspects of the cybersecurity challenge



OUTCOME:

Build a practical, usable, repeatable implementation to address the cybersecurity challenge

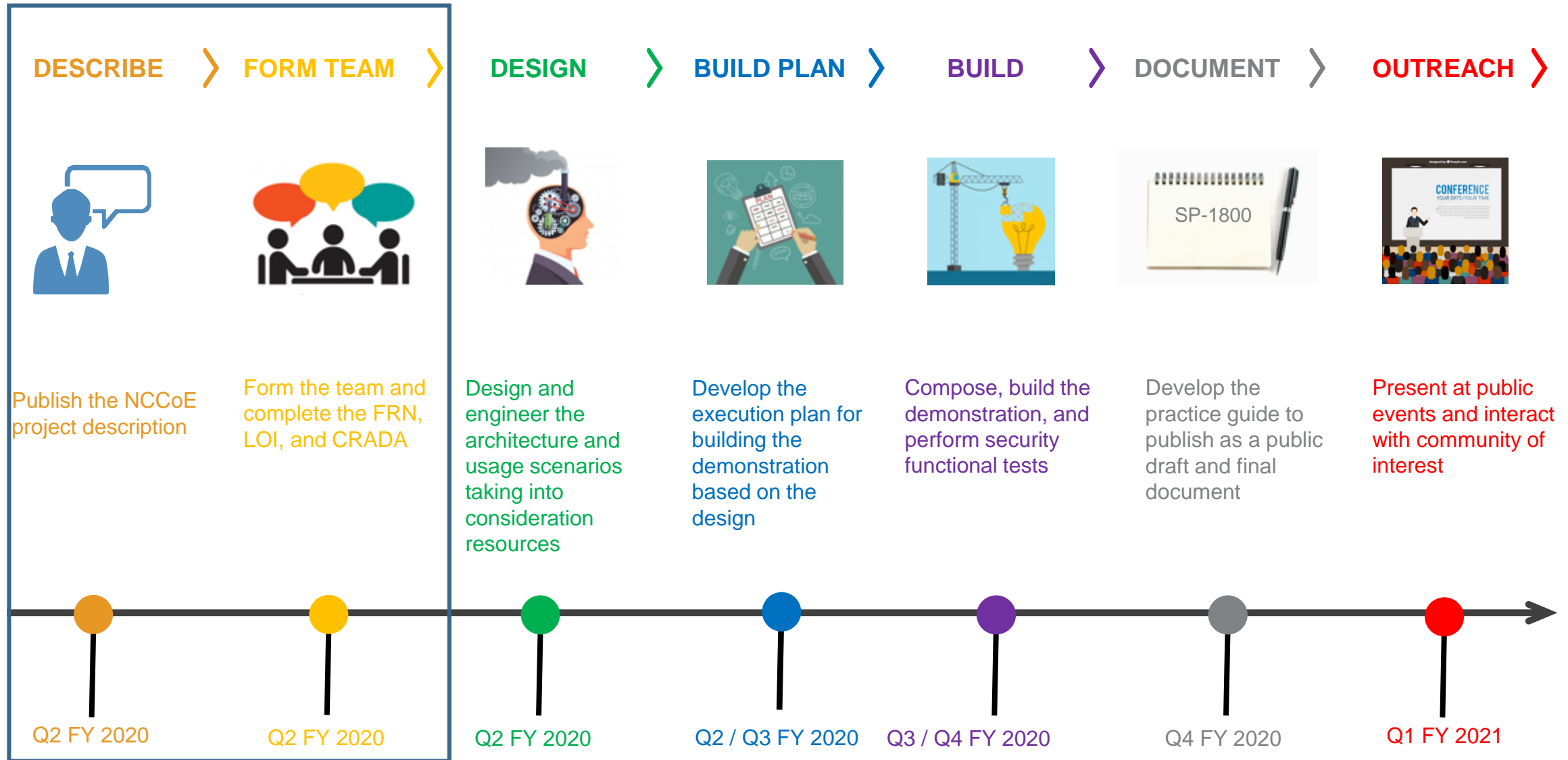


OUTCOME:

Advocate adoption of the example implementation using the practice guide

Project Execution Timeline

Detecting and Protecting Against Data Integrity Attacks in ICS Environments

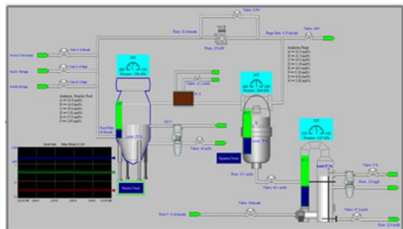


Detecting and Protecting Against Data Integrity Attacks in Industrial Control Systems (ICS) Environments

Challenge

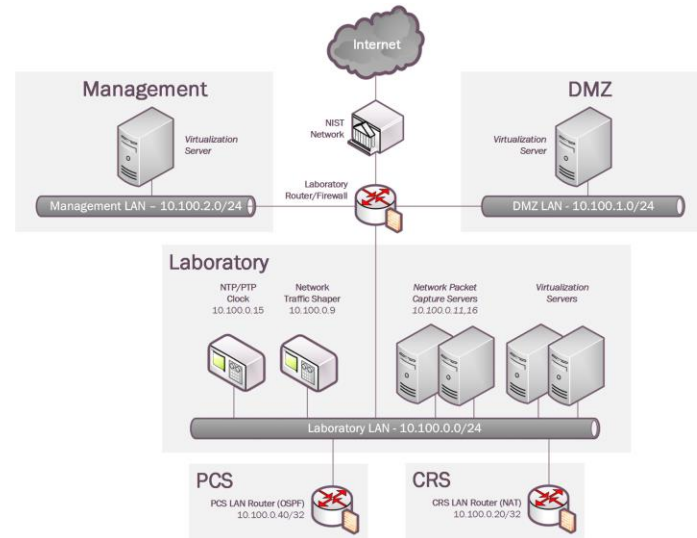
- ICS are used in manufacturing to aid automation and reliability
- There is potential for increased cyber incidents as ICS become more connected to the internet
- Traditional IT malware can disrupt industrial environments by altering the information and system integrity in ICS
- To enhance system security, manufacturing organizations must be able to detect and protect against system and information-integrity attacks

Operational
Technology



Information
Technology

Goals



- Provide a comprehensive approach to prevent, detect, and mitigate cyber and insider threats within discrete and process manufacturing environments
- Provide a proposed approach to detect misconfigurations and device faults
- Demonstrate how manufacturing organizations can use commercially available technologies to secure their operational technology systems

Benefits

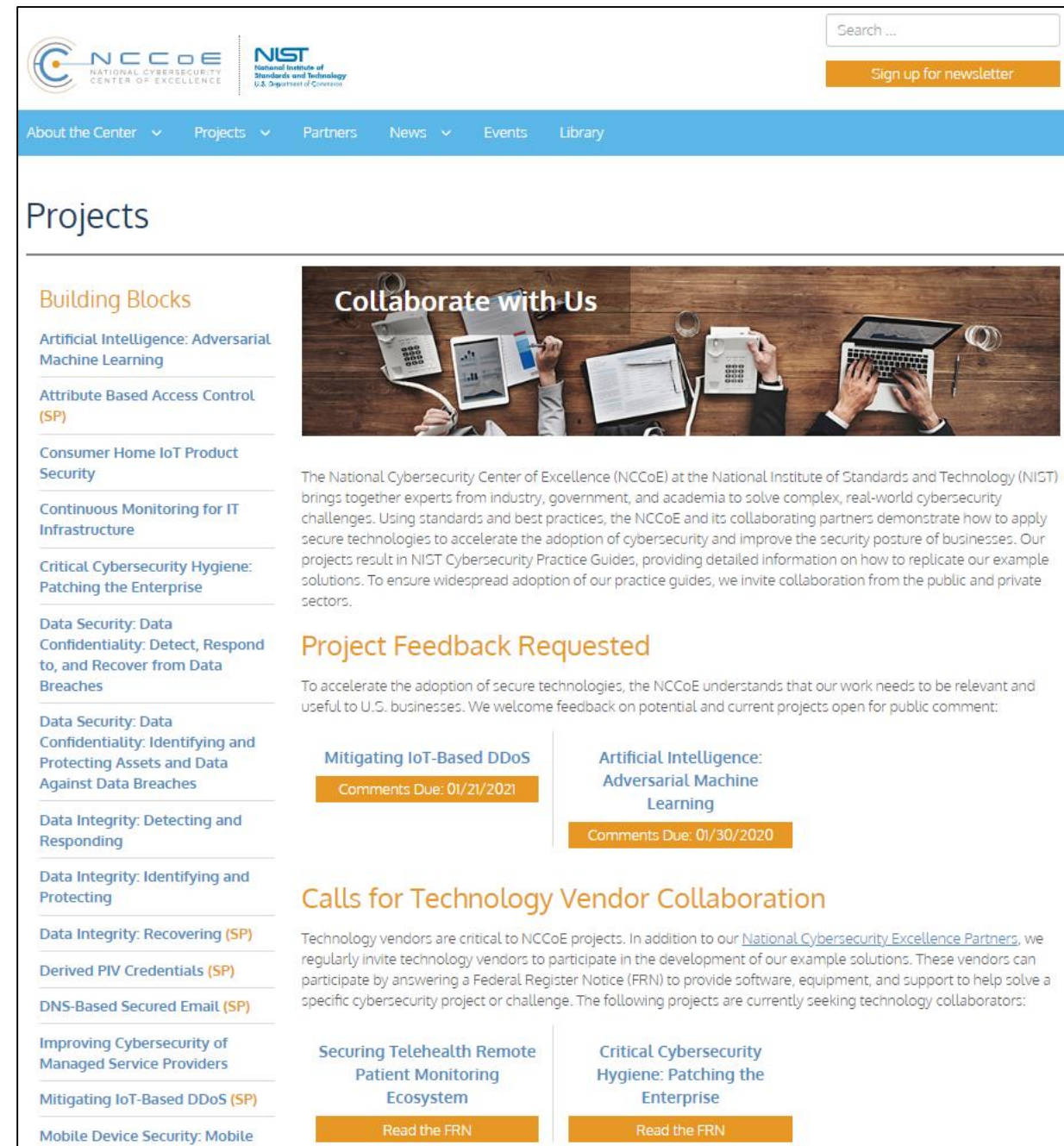
- Detect and prevent unauthorized software installation
- Protect computers and ICS networks from potentially harmful applications
- Determine changes made to a network using change management tools
- Detect unauthorized use of systems
- Continuous monitoring of networks
- Malware detection and mitigation



Collaborate with us

Respond to a Federal Register Notice (FRN): <https://nccoe.nist.gov/projects>

- Our web page will have a link to released FRN
- Desired technology components are listed in FRN
- Respond to an FRN by submitting a Letter of Intent
- We'll review LOI on a first come, first serve basis
- Accepted collaborators will be asked to sign a Cooperative Research and Development Agreement (CRADA) with NIST



The screenshot shows the 'Projects' page of the National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST). The page features a blue header with navigation links: 'About the Center', 'Projects', 'Partners', 'News', 'Events', and 'Library'. A search bar and a 'Sign up for newsletter' button are in the top right. The main content area is titled 'Projects' and includes a 'Building Blocks' section with a list of project topics: Artificial Intelligence: Adversarial Machine Learning, Attribute Based Access Control (SP), Consumer Home IoT Product Security, Continuous Monitoring for IT Infrastructure, Critical Cybersecurity Hygiene: Patching the Enterprise, Data Security: Data Confidentiality: Detect, Respond to, and Recover from Data Breaches, Data Security: Data Confidentiality: Identifying and Protecting Assets and Data Against Data Breaches, Data Integrity: Detecting and Responding, Data Integrity: Identifying and Protecting, Data Integrity: Recovering (SP), Derived PIV Credentials (SP), DNS-Based Secured Email (SP), Improving Cybersecurity of Managed Service Providers, Mitigating IoT-Based DDoS (SP), and Mobile Device Security: Mobile. To the right, there is a large banner titled 'Collaborate with Us' with an image of people working on laptops. Below the banner, a paragraph describes the NCCoE's mission and the importance of collaboration. A section titled 'Project Feedback Requested' encourages public input on specific projects, with 'Mitigating IoT-Based DDoS' having a comment deadline of 01/21/2021 and 'Artificial Intelligence: Adversarial Machine Learning' having a deadline of 01/30/2020. At the bottom, a section titled 'Calls for Technology Vendor Collaboration' invites vendors to participate in the development of example solutions, with specific projects like 'Securing Telehealth Remote Patient Monitoring Ecosystem' and 'Critical Cybersecurity Hygiene: Patching the Enterprise' highlighted with 'Read the FRN' buttons.

Collaborate with Us

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) brings together experts from industry, government, and academia to solve complex, real-world cybersecurity challenges. Using standards and best practices, the NCCoE and its collaborating partners demonstrate how to apply secure technologies to accelerate the adoption of cybersecurity and improve the security posture of businesses. Our projects result in NIST Cybersecurity Practice Guides, providing detailed information on how to replicate our example solutions. To ensure widespread adoption of our practice guides, we invite collaboration from the public and private sectors.

Project Feedback Requested

To accelerate the adoption of secure technologies, the NCCoE understands that our work needs to be relevant and useful to U.S. businesses. We welcome feedback on potential and current projects open for public comment:

- Mitigating IoT-Based DDoS**
Comments Due: 01/21/2021
- Artificial Intelligence: Adversarial Machine Learning**
Comments Due: 01/30/2020

Calls for Technology Vendor Collaboration

Technology vendors are critical to NCCoE projects. In addition to our [National Cybersecurity Excellence Partners](#), we regularly invite technology vendors to participate in the development of our example solutions. These vendors can participate by answering a Federal Register Notice (FRN) to provide software, equipment, and support to help solve a specific cybersecurity project or challenge. The following projects are currently seeking technology collaborators:

- Securing Telehealth Remote Patient Monitoring Ecosystem**
Read the FRN
- Critical Cybersecurity Hygiene: Patching the Enterprise**
Read the FRN

➤ Additional Ways to Collaborate

Sign-up for email updates: <https://public.govdelivery.com/accounts/USNIST/subscriber/new>

Join a Community of Interest: https://nccoe.nist.gov/about_the_center/coi

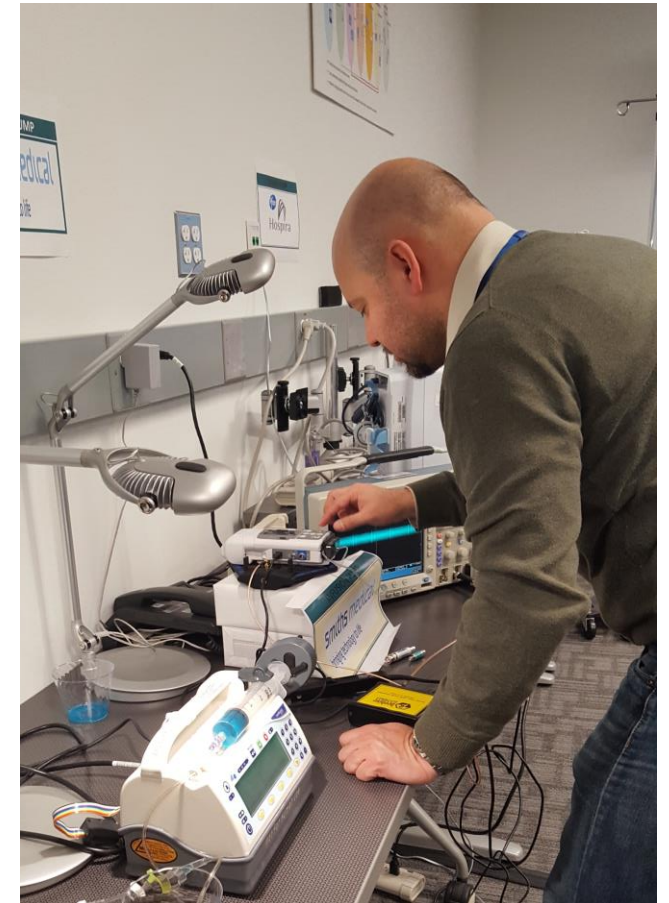
Submit a project idea: <https://nccoe.nist.gov/projects>

Attend an event: <https://nccoe.nist.gov/events>

Submit comments on drafts: <https://nccoe.nist.gov/projects>

Respond to an FRN: <https://nccoe.nist.gov/projects>

Share adoption stories: nccoe@nist.gov



David Stieren

Manufacturing Extension Partnership



Division Chief for Extension Services

David Stieren is the Division Chief for Extension Services at NIST MEP. He oversees a division that works with MEP Centers, U.S. manufacturers, NIST Laboratories, other government agencies, and other stakeholders to develop and deploy approaches that are used by the National Network of MEP Centers to provide extension services to U.S. manufacturers. The NIST MEP Extension Services Division focus is the provision of National-level guidance and resources to MEP Centers as they provide technical and business assistance to U.S. manufacturers to help them grow and compete in the global marketplace.

> Questions? Contact Us



Michael Powell

Federal Lead: Manufacturing Sector

Michael.Powell@nist.gov

301-975-0310

Titilayo Ogunyale

Project Lead: Manufacturing Sector

Togunyale@mitre.org

301-975-0219

Project email: manufacturing_nccoe@nist.gov



<http://nccoe.nist.gov>



301-975-0200



nccoe@nist.gov

The NIST Hollings Manufacturing Extension Partnership (MEP) Program

**NIST Cybersecurity Center of
Excellence (NCCOE)
Manufacturing Community of
Interest Webcast**

January 23, 2020

NIST MEP Participants

- **David Stieren**
Division Chief, Extension Services
david.stieren@nist.gov
- **Pat Toth**
Cybersecurity Services Manager
patricia.toth@nist.gov



MEP National Network



Non-federal assistance
Centers located in all 50
US states and Puerto Rico,
program managed by NIST



Public-private partnership
with local flexibility



Federal funds, state investments,
private sector fees cover services

- \$146M FY20 NIST MEP;
matched by MEP Centers



Market driven program that
creates high value for
manufacturers



Leverage partners to
maximize service offerings



Extension-based program
transfers technology and
expertise to manufacturers

MEP National Network





NATIONAL NETWORK

One Center in
Every State and
Puerto Rico

Nearly

2,100



Service
Providers
& Partners

Over

1,400



Manufacturing
Experts

Approx.

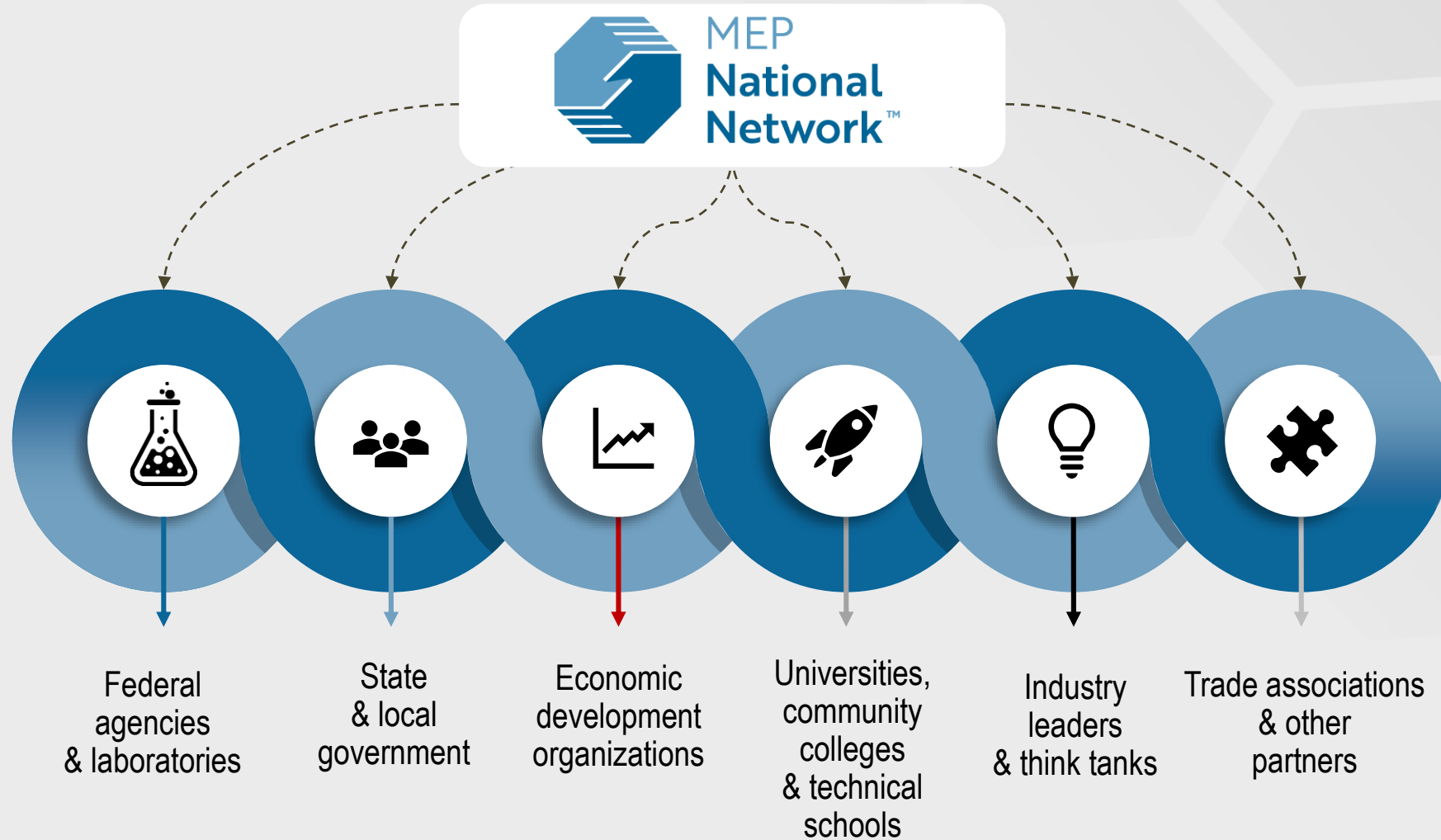
375



Service
Locations



Our Partners





Manufacturing USA + MEP National Network





*In FY2019, the MEP National
Network connected with 28,213
manufacturers, leading to:*

114,650 JOBS Created or Retained

**\$15.7
BILLION**
in New and
Retained Sales



**\$4.5
BILLION**
in Total Investment in
U.S. Manufacturing



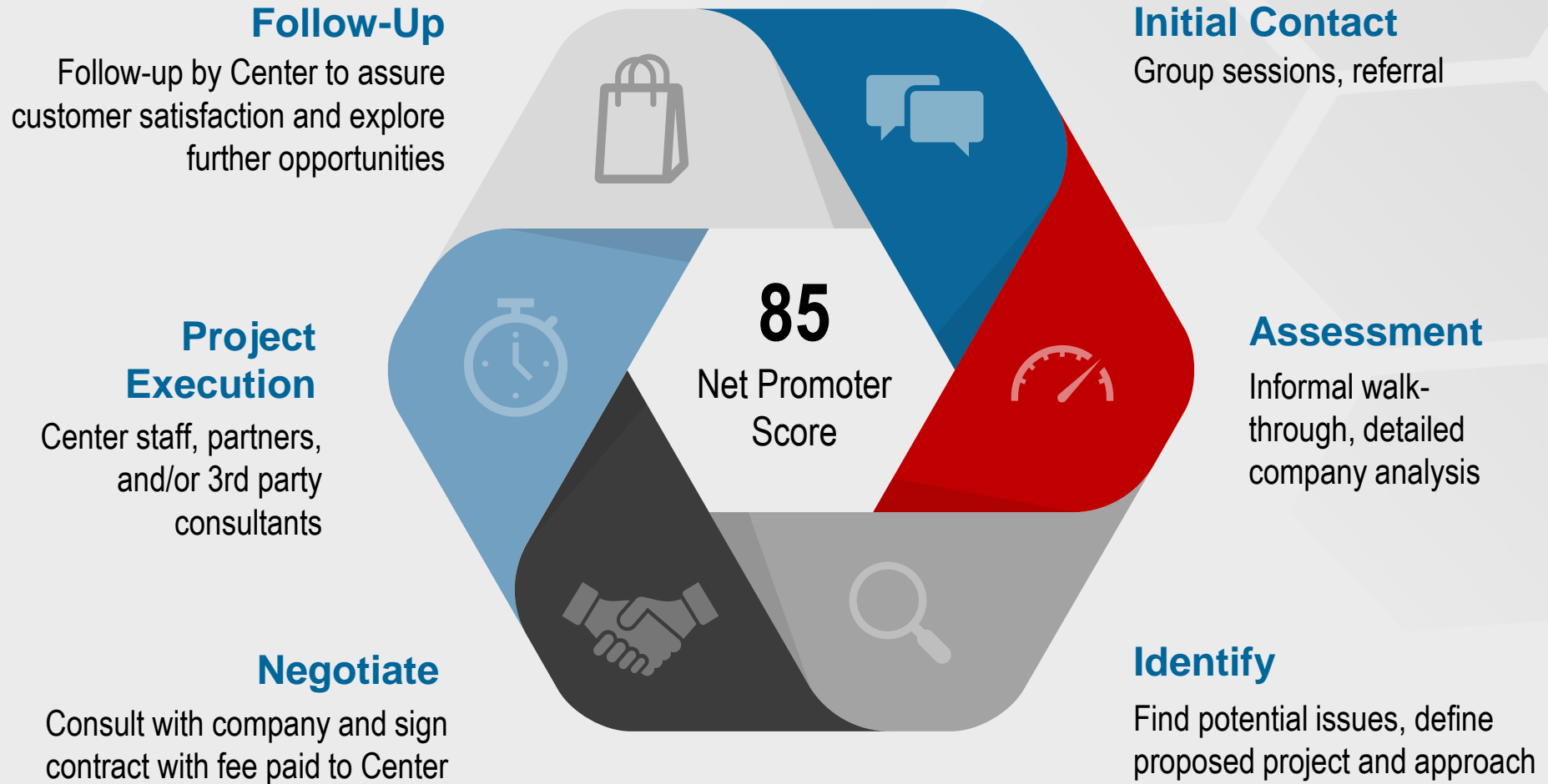
**\$1.5
BILLION**
in Cost
Savings



Numbers are based on survey results from MEP Center clients.



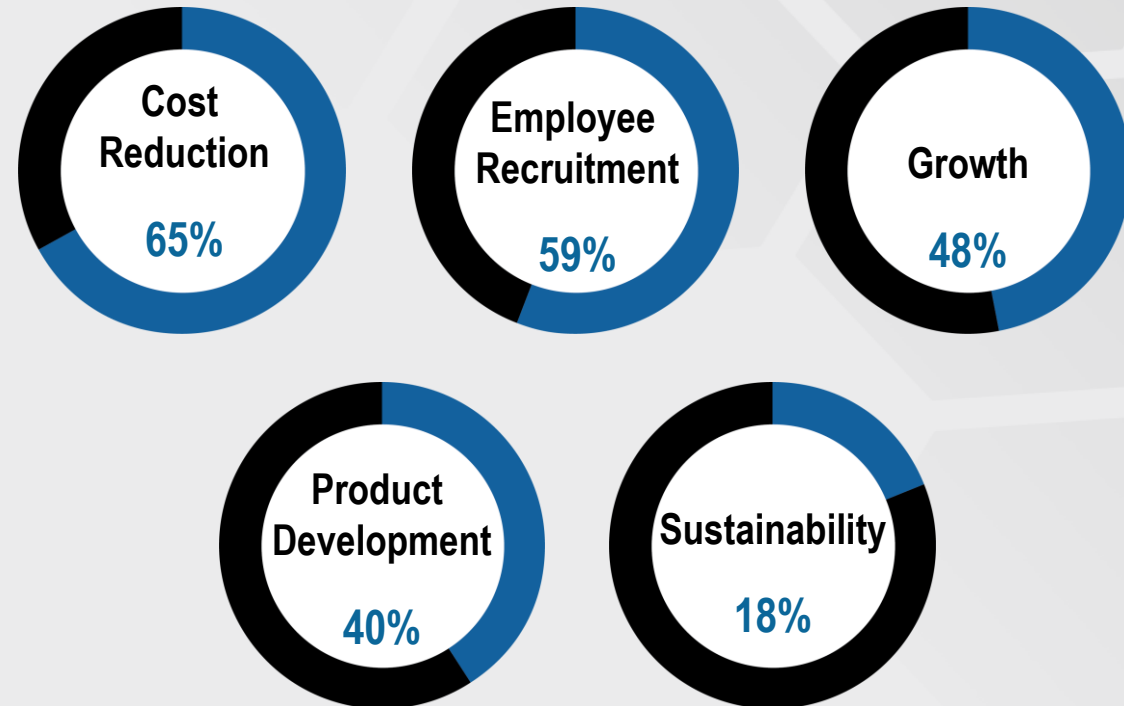
How Centers Work with Manufacturers



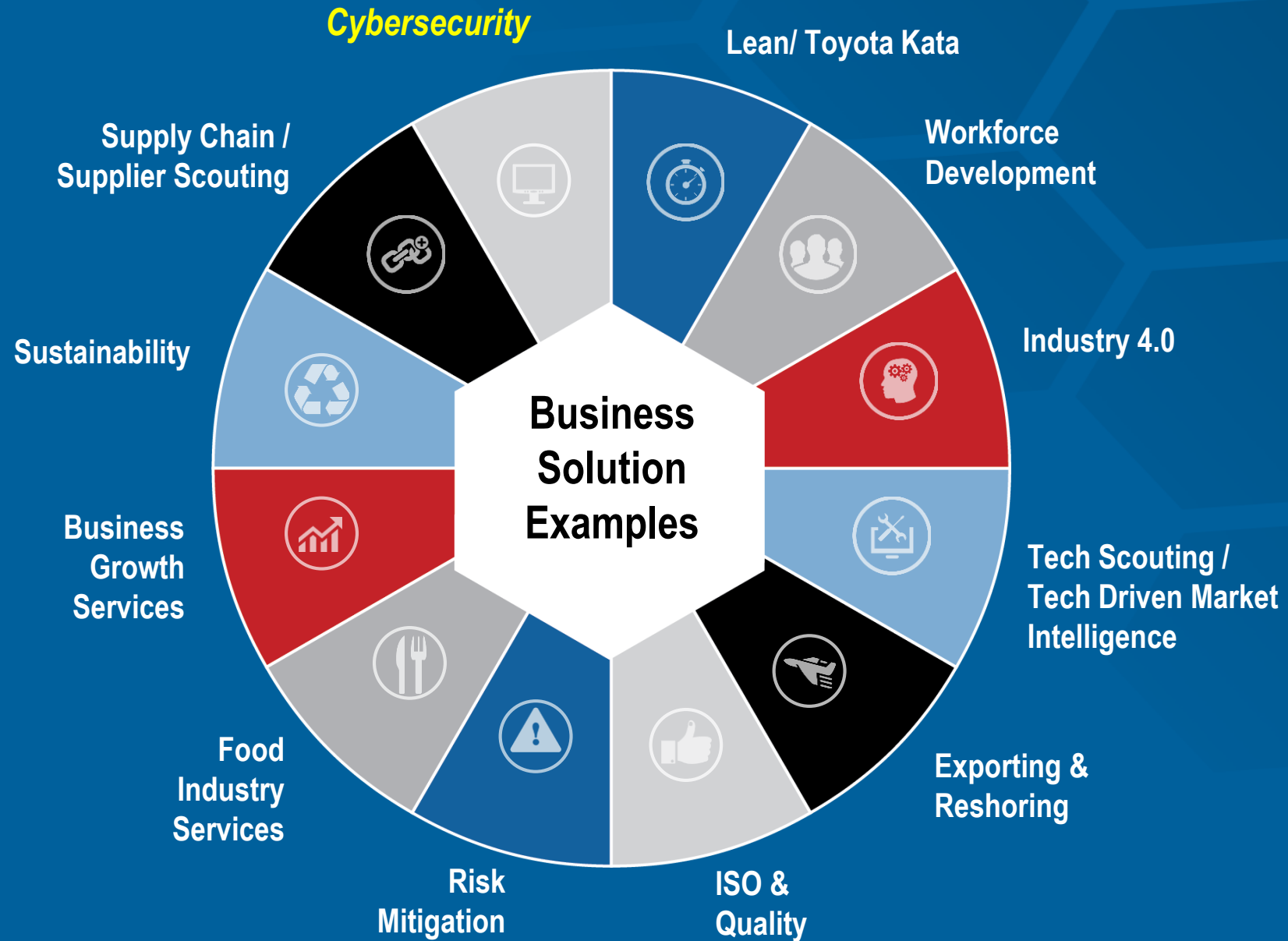


Client Challenges

The share of MEP clients reporting **employee recruitment and retention** as a challenge has nearly **tripled**.



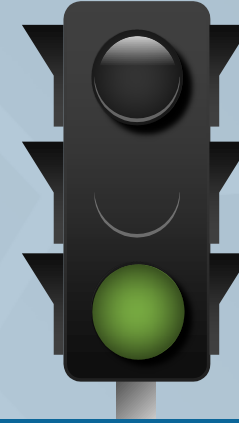
Information based on FY 2019 MEP National Network Client Impact Survey





MEP National Network Cybersecurity Summary

- MEP National Network cybersecurity assistance for small manufacturers available via MEP Centers nationwide in 2020
- Spurred by strong partnerships with DoD and mainly driven by Defense Federal Acquisition Regulation Supplement (DFARS) requirements for defense sector
- Small U.S. manufacturers not showing significant action for cybersecurity implementation in non-defense industries
 - ✓ *Small manufacturer cyber protections low relative to larger companies*
 - ✓ *MEP working with non-defense supply chains, e.g., auto, food mfg, others*
- MEP National Network engaging NIST Labs relating to cyber protections for manufacturing operational technology

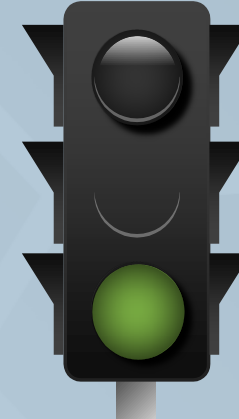


MEP Centers
Nationwide
participating in MEP
NN Working Group



MEP National Network Cybersecurity Summary

- Cybersecurity for Defense Manufacturers
 - ✓ Applying DoD Funding via Interagency Agreement between NIST MEP and Office of Secretary of Defense
 - ✓ 30+ Awareness Events across the country this year, targeting ~1,000 small defense contractors
 - ✓ 10 companies selected for Assessments and technical assistance regarding DFARS-required cyber protections
 - ✓ CSF Manufacturing Profile Implementation Guidance
 - 2 use cases provide to NIST Lab from defense contractor MEP Center clients
- MEP Resources
 - ✓ NIST Handbook 162
 - ✓ <https://www.nist.gov/mep/cybersecurity-resources-manufacturers>



30+ Awareness events
in 2020 targeting 1,000
defense contractors



Questions / Discussion

NIST MEP Contact Info

- David C. Stieren
Division Chief, Extension Services
david.stieren@nist.gov
- Pat Toth
Cybersecurity Services Manager
patricia.toth@nist.gov
- www.nist.gov/mep