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**

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

**ASSEMBLE**

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

**BUILD**

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

**ADVOCATE**

**OUTCOME:** Advocate adoption of the example implementation using the practice guide
# Project Execution Timeline

## Detecting and Protecting Against Data Integrity Attacks in ICS Environments

<table>
<thead>
<tr>
<th>Stage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DESCRIBE</strong></td>
<td>Publish the NCCoE project description</td>
</tr>
<tr>
<td><strong>FORM TEAM</strong></td>
<td>Form the team and complete the FRN, LOI, and CRADA</td>
</tr>
<tr>
<td><strong>DESIGN</strong></td>
<td>Design and engineer the architecture and usage scenarios taking into consideration resources</td>
</tr>
<tr>
<td><strong>BUILD PLAN</strong></td>
<td>Develop the execution plan for building the demonstration based on the design</td>
</tr>
<tr>
<td><strong>BUILD</strong></td>
<td>Compose, build the demonstration, and perform security functional tests</td>
</tr>
<tr>
<td><strong>DOCUMENT</strong></td>
<td>Develop the practice guide to publish as a public draft and final document</td>
</tr>
<tr>
<td><strong>OUTREACH</strong></td>
<td>Present at public events and interact with community of interest</td>
</tr>
</tbody>
</table>

### Project Execution Timeline

<table>
<thead>
<tr>
<th>Stage</th>
<th>Timeline</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q2 FY 2020</td>
<td></td>
</tr>
<tr>
<td>Q2 FY 2020</td>
<td></td>
</tr>
<tr>
<td>Q2 FY 2020</td>
<td></td>
</tr>
<tr>
<td>Q2 / Q3 FY 2020</td>
<td></td>
</tr>
<tr>
<td>Q3 / Q4 FY 2020</td>
<td></td>
</tr>
<tr>
<td>Q4 FY 2020</td>
<td></td>
</tr>
<tr>
<td>Q1 FY 2021</td>
<td></td>
</tr>
</tbody>
</table>

---

National Cybersecurity Center of Excellence  
nccoe.nist.gov
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

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
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 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

- Federal agencies & laboratories
- State & local government
- Economic development organizations
- Universities, community colleges & technical schools
- Industry leaders & think tanks
- Trade associations & other 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

Initial Contact
Group sessions, referral

Assessment
Informal walk-through, detailed company analysis

Identify
Find potential issues, define proposed project and approach

Negotiate
Consult with company and sign contract with fee paid to Center

Project Execution
Center staff, partners, and/or 3rd party consultants

Follow-Up
Follow-up by Center to assure customer satisfaction and explore further opportunities

85 Net Promoter Score

Project impact data collected by contractor for NIST approximately 6-12 months after project completion
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 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