National Defense Industrial Association

Cybersecurity for Advanced Manufacturing Joint Working Group (CFAM)

Policy Planning and Impacts (PPI) Team

Agenda

- Team Introductions
- Deliverable
- Approach
- Interview List
- Next Steps

Team Introductions

Team Members:

- **Megan Brewster**
- **Martha Charles-Vickers**
- **Jason Gorey**
- **Daryl Haegley**
- **Tom McDermott**
- **Joe Spruill**
- ***Sarah Stern (Team Leader)***
- **Bill Trautmann**
- **Melinda Woods**

Integration Team Participants:

- **Donald Davidson**
- **Larry John**
- **Michele Moss**
- **Kaye Ortiz**
- **Chris Peters**
- **Melinda Reed**
- **Stephanie Shankles**

Deliverable

- Our deliverable is a report analyzing the existing policies, standards, best practices and regulations in the manufacturing environment (as defined by the CFAM Manufacturing Environment Team) that can mitigate cyber risks. Our report will identify relevant initiatives addressing cybersecurity, gaps where additional protection is needed, and will recommend actions to address those gaps. The report will also provide recommendations on breach reporting, communication processes and what is practical for industry. The report will answer the following questions posed in the CFAM terms of reference.
- What existing policies regulations, and standards are applicable to cybersecurity in advanced manufacturing? How do existing policies, regulations and standards need to be augmented, and by whom?
  - This includes identifying efforts which may be under development to address the defined actions, and a gap analysis identifying areas of interest for future efforts.
- How can existing network breach reporting and communication processes be improved to increase cybersecurity in manufacturing environments, and by whom?
  - Case Studies will be included, if available.
- What activities implemented by government agencies outside the Department of Defense or by the private sector can be leveraged to better protect manufacturing networks?

Approach

- **Analyze:**
  - **Applicability of existing policies, regulations, and standards**
  - **Gaps in policies, regulations, and standards**
  - **Case studies of network breach reporting and communication processes**
  - **Constraints on industry and the government**
  - **Breakdown of current activities on the protection of manufacturing networks**

- **Develop:**
  - **Recommendations on how policies, regulations, and standards need to be augmented**
  - **Recommendations on best practices of breach reporting, and communication processes**

Interview List

- National Cybersecurity Center of Excellence (NCCoE)
- NIST Cybersecurity Framework Office (Matthew Barrett)
- Industrial Control Systems-Cyber Emergency Response Team (ICS-CERT)
- Office of DoD CIO – Defense Industrial Base Cybersecurity (Vicki Michetti)
- OUSD/Defense Procurement and Acquisition Policy (Rose Bartlett)
- DoD Defense Standardization Program Office (Greg Saunders)
- Trustworthy Suppliers Framework (Dr Brian Cohen)
- Aerospace Industry Association (Rusty Rensch and Gery Mras)
- Robert Metzger, esquire
- FireEye Government Best Practices Panelists (or staff):
  - Michael K. Daly, CTO, Raytheon Company
  - Michael Echols, CISO for Maricopa County
  - Mike Roling, CISO, State of Missouri
  - Darren Van Booven, CISO, Idaho National Lab

Next Steps

- Obtain good understanding of policy, standards and best practices landscape
- Identify SMEs
- Schedule SME interviews
- Develop test cases to synthesize findings and identify gaps
- Develop recommendations