NDIA Cybersecurity for Advanced Manufacturing Public Forum

August 18, 2016

Policy, Planning & Impacts Team

Ms. Stephanie Shankles
for team leader
Ms. Sarah Stern

Policy Planning & Impacts Team

- **Team Lead: Sarah Stern, Boeing BCA Network Cyber Security**

Megan Brewster OSTP	**Daryl Haegley** OASD (EI&E) IE	**Melinda Reed** ODASD(SE)	**Stephanie Shankles** Contract support to DOD Office of CIO
Martha Charles-Vickers Sandia National Laboratories	**Thomas McDermott** Georgia Tech Research Institute	**Joseph Spruill** Lockheed Martin Corporation	**Bill Trautmann** JSJ4, KBLD
Donald Davidson Office of the DoD CIO	**Michele Moss** Contract support to DOD Office of CIO	**Sarah Stern** Boeing, BCA Network Cyber Security	**Melinda Woods** AT&L MIBP
Jason Gorey Six O'Clock Ops			

Objective

- Assess existing policies and regulations for applicability to CFAM; will determine additional administrative actions that could strengthen manufacturing cybersecurity, and will assess breach reporting and communication processes for improvements.

- Our goal is to learn what is needed and engage both sides of the manufacturing floor in order to propose policy to the DoD to direct best cyber security practice in the advanced manufacturing environment.

Current Status

On-going activities:

- Developed subcommittees to address key components of the report
- Developed deliverable statements of work
- Started Cyber Policy/Regulation Gap analysis
- Created a cyber security survey for the NDIA members in Cyber and Manufacturing
- Gathered a list of interviewees that are SMEs in Cyber or Manufacturing
  - Conducted 1 interview this month
- Researching current cyber law which impacts breach reporting

SME input needed:

- NIST SME
- Manufacturing Floor input– guidance, standards, best practices, etc.
- Security industry SME that specializes in information security for manufacturing

Issue 1: Protection of IP Confidentiality and Integrity During Advanced Manufacturing

DOD Acquisition Policy
- Risk Management Framework
- Program Protection Planning

DoD Operation Policy – is this applicable to contractors?
- STIGS
- Continuous Diagnostics and Monitoring

DoD IT networks
DoD programs & systems

Requirements for Prime Contractors
- Federal Regulations & DFARS
- Safeguarding DFARs – including NIST SP800-171
- Voluntary DIB CS Program
- Contract specific requirements
- Required Accreditations (FEDRamp, NIAP)

Can we define the Safeguarding DFAR that requires implementing NIST SP800-171 controls for CDI as the only requirement that reaches the manufacturing floor? How does it flow past the prime?

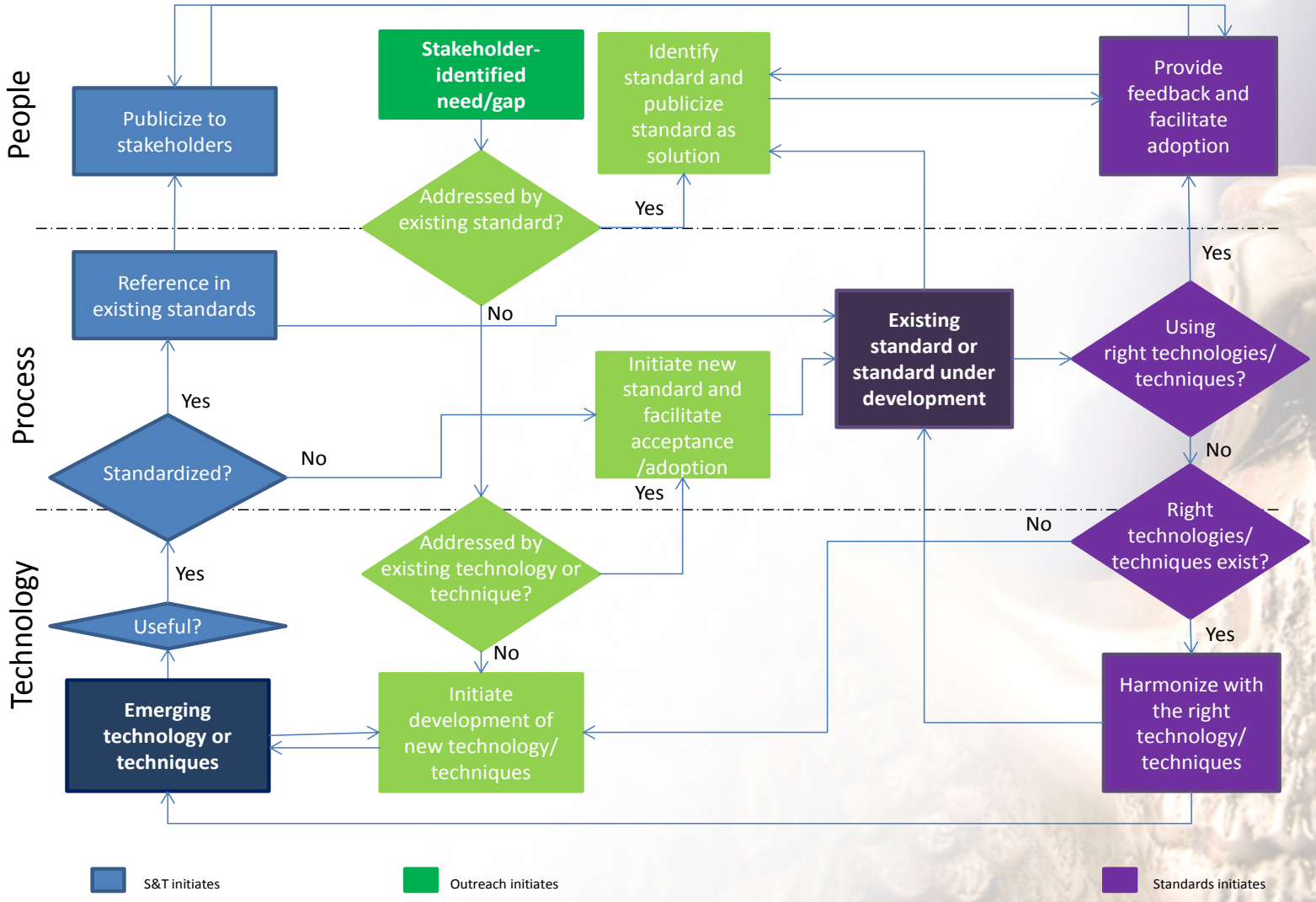
Voluntary Adoption of Security and Cybersecurity
- Cybersecurity Framework
- NIST SP 800-82
- NIST SP 800-53

Advanced Manufacturing Floor
- **What is required for government owned, contractor owned, and commercial**

A GAP exists between DOD Acquisition Policy and Required Protections During Advanced Manufacturing

National Defense Industrial Association

Standards Development Process Flow



Back up slides

PPI Team Tasking

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?

Resources

- Http://www.acq.osd.mil/dpap/dars/dfars/html/current/204_73.htm
  link for actual DFAR Language
- http://www.acq.osd.mil/dpap/pdi/docs/FAQs_Network_Penetration_Reporting_and_Contracting_for_Cloud_Services.pdf
  link for FAQ sheet on new DFAR language / reqt
- http://www.acq.osd.mil/se/docs/DFARS-guide.pdf
  DoD Guidance on implementing DFAR language ref CUI
- https://www.dauaa.org/Web2011/PDFiles/igatingUnclassifiedInformationSystemSecurityProtections.pdf
- What DAU is teaching--- listed as UNCLASS
- http://www.hlregulation.com/2016/01/07/dod-amends-its-dfars-safeguarding-and-cyber-incident-reporting-requirements-with-a-second-interim-rule/
  Recent News Article
- http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf
  NIST SP 800-171 on Protecting CUI
- The primary statutes to cite are the Federal information Security Management Act (PL 107-347 - Title 3) and Clinger Cohen Act. Together they --
  - Establishes the role of the Agency CIOs
  - Sets responsibilities for information system/information security Standards (e.g., Section 11331 of Title 40 states that standards proposed by NIST shall include standards that provide minimum information security requirements, which shall be compulsory and binding.
  - It gives heads of agency the authority to employ more stringent standards
  - and more.
- This page on NIST cite does a good job summarizing...http://csrc.nist.gov/groups/SMA/fisma/overview.html
- You can find related authorities for NSS standards on the CNSS website; however they are through executive orders/directives and not statute.