Cybersecurity For
Advanced Manufacturing Forum

CFAM Policy, Planning and Impacts Team

Ms. Sarah Stern, Boeing
Team Lead

Lockheed Martin
Global Vision Center
Arlington, VA

November 15, 2016

Policy Planning & Impacts Team

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

Introduction

The Policy, Planning & Impacts (PPI) Team focused on the manufacturing networks and the protection of the digital thread data, analyzing:

- Applicability of existing policies, regulations, and standards
- Gaps in policies, regulations, and standards
- Survey of network breach reporting and communication processes
- Breakdown of current activities on the protection of manufacturing networks

The PPI white paper objectives were to provide recommendations on:

- How policies, regulations, and standards need to be augmented
- Best practices of breach reporting, and communication processes

Introduction

Multiple descriptions of covered information exist, including:

Covered Defense Information (CDI)

Unclassified Controlled Technical Information (UCTI)

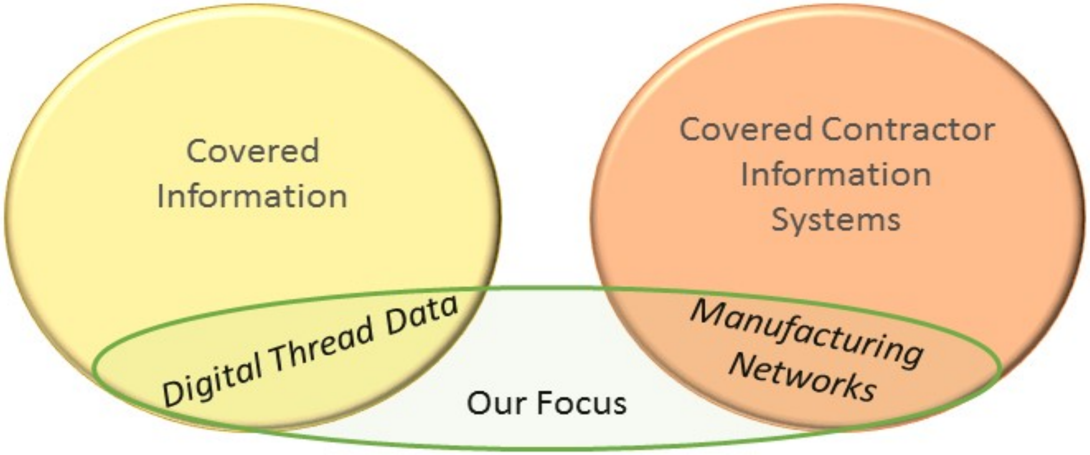
Controlled Technical Information (CTI)

Controlled Unclassified Information (CUI)

For our study, we have used CDI as a standard nomenclature.

“Safeguarding Covered Defense Information and Cyber Incident Reporting” DFARS SUBPART 204.73

“Network Penetration” DFARS 252.204-7008 and 252.204-7012



Focus on:

- Operational technology networks and interfaces, not IT or enterprise networks
- Manufacturing cyber environment, not general cybersecurity

Discussion

Through our research to identify existing policies, regulations, and standards that addresses cybersecurity on the manufacturing floor, we found:

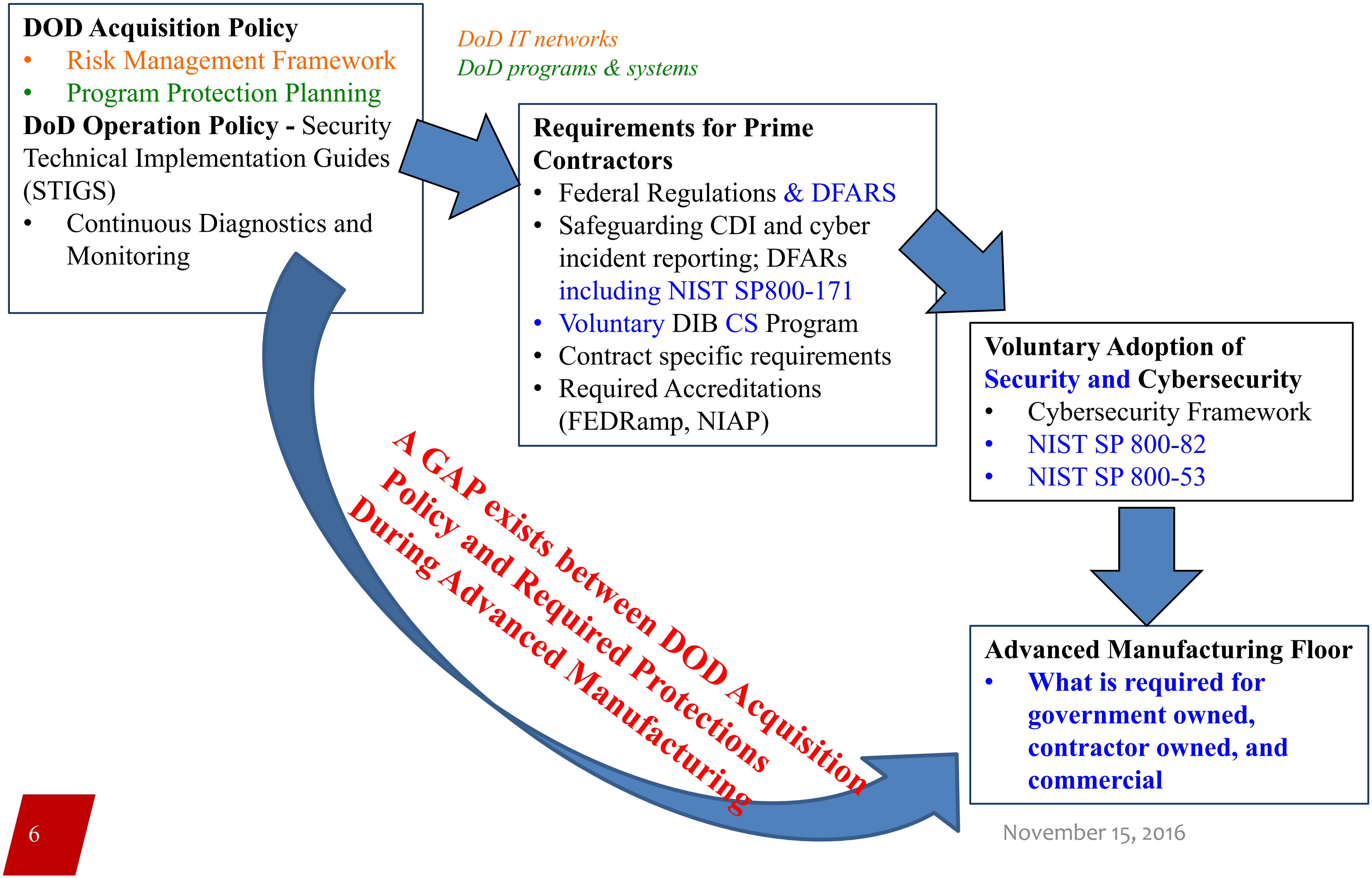
- A gap of applicable policies, regulations or standards that directly addresses the factory floor networks' security
- A challenge to develop policy to fill the gap in the hyper-dynamic cybersecurity environment
- An opportunity to modify or amend existing guidance to more expeditiously protect manufacturing networks

Some guidance that may be able to be adapted to more directly apply to the manufacturing OT environment are:

- NIST SP 800-171
- DFARS 252.204-7008
- DFARS 252.204-7012
- DFARS Subpart 204-73
- NIST Cybersecurity framework
- NIST IR 8099 - Smart Manufacturing

A combination of requirements with incentives and voluntary best practices appears to be the leanest, most adaptable way to manage the ever changing factory floor OT environment

Protection of IP Confidentiality and Integrity During Advanced Manufacturing



DOD Acquisition Policy

- Risk Management Framework
- Program Protection Planning

DoD Operation Policy - Security Technical Implementation Guides (STIGS)

- Continuous Diagnostics and Monitoring

DoD IT networks

DoD programs & systems

Requirements for Prime Contractors

- Federal Regulations & DFARS
- Safeguarding CDI and cyber incident reporting; DFARs including NIST SP800-171
- Voluntary DIB CS Program
- Contract specific requirements
- Required Accreditations (FEDRamp, NIAP)

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

Findings

- No policy/regulation/standards coverage for the manufacturing OT environment for cybersecurity . . . *guidance that applies to the IT environment may be able to be adapted to the OT environment*

- Breach reporting data is currently hindered by companies concerned with sharing their data . . . *unless companies feel comfortable with the process for sharing this information, we will not be able to better learn about trends in attacks*

- The manufacturing industry is starting initiatives to look at the issue of cybersecurity in manufacturing OT . . . *while there is strength in numbers, we need to ensure the message being communicated is consistent*

Recommendations

Recommendation 1: Office of Assistant Secretary of Defense for Systems Engineering (OASD(SE)) should amend guidance, templates and references for Program Protection Planning to require Program Managers to identify and protect important data that adversaries and/or competitors can exploit, including, but not necessarily limited to, design data, product specifications, process control data, and test data. Specifically, modify:

- The "Expectations" paragraph accompanying para. 3.1 (and other locations as needed) in DoD's *Program Protection Plan Outline & Guidance* document to add manufacturing specialists as key participants in the CPI identification process.
- Corresponding locations in DoD's *Program Protection Plan Evaluation Criteria* document.
- Chapter 13 of the *Defense Acquisition Guidebook*
- *Engineering for System Assurance,* published by NDIA in cooperation with DoD.

Recommendations

Recommendation 2: OASD(R&E) and OASD(L&MR) should create, or add to, existing DoD-sponsored academic research programs, focused research efforts designed to discover vulnerabilities within existing and emerging manufacturing networks.

- Program could be executed by an existing DoD-sponsored University Affiliated Research Center (UARC) like the Systems Engineering Research Center (SERC).

Recommendation 3: Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (USD/AT&L) should issue guidance that clarifies the extent of the requirements flowdown within the context of DFARS SUBPART 204.73, DFARS 252.204-7008, and DFARS 252.204-7012.

- NDIA would be willing to work with DoD to create and execute a series of workshops designed to highlight and assess tradeoffs in this area.

Questions and Discussion