Cybersecurity for Advanced Manufacturing: Understanding the Digital Thread

Presented to: NDIA’s Cybersecurity for Advanced Manufacturing Forum
Presenter: Larry John, ANSER (Larry.John@anser.org)
Date: 15 November 2016
Manufacturing Concerns:

- Theft of technical info -- can compromise national defense and economic security
- Alteration of technical data -- can alter the part or the process, with physical consequences to mission and safety
- Disruption or denial of process control -- can shut down production

A risk management problem. Need resilience!
CFAM JWG Objective

Government and industry members of the CFAM JWG collaborate to build on recommendations in the 2014 NDIA white paper, *Cybersecurity for Advanced Manufacturing*

- Identify cybersecurity vulnerabilities in the manufacturing environment and mitigations... *types and boundaries, highest impact near-term actions, culture changes*
- Identify ways to incentivize and assist manufacturers to improve cybersecurity in manufacturing systems... *policies and contract requirements, security practices, workforce cybersecurity training*
- Develop implementation plans... *coordinated with government and industry groups*
Focus Area

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

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

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.

Focus on:
- Operational technology networks and interfaces, not IT or enterprise networks
- Manufacturing cyber environment, not general cybersecurity
Operational Technology (OT) vs. IT
What’s Different?

• ICS systems are long-lived capital investments (15-20 year life)
  – Obsolete operating systems and software are common
  – New systems architected for security, but hard to interoperate with old

• “Production mindset” with little tolerance for OT down time
  – Operate in real time with critical safety implications – cannot install patches without scheduled downtime and testing
  – Nascent cybersecurity awareness and limited workforce training.

• Manufacturing differs from other ICS applications (e.g. Power Grid)
  – Every manufacturing job brings new executable code into system
  – Tech data flowing through the system is a target

November 15, 2016
Modern Manufacturing

- Manufacturing is an increasingly digital business
  - Smart Manufacturing
  - Industrial Internet of Things
  - Industry 4.0
  - ...

- Advanced Manufacturing is:
  - **Networked** at every level to gain efficiency, speed, quality and agility
  - **Constantly learning** from models and data throughout the life cycle
  - **Driven by a “Digital Thread”** of product and process information
    - Source of competitive advantage for manufacturers and their customers
    - Source of military advantage for DoD
    - Demands protection throughout the product lifecycle
  - **Has a “Digital Twin”** (models and simulations) used to mirror and predict activities and performance of processes and products
## NDIA Division Representation

### Cyber
- **Dawn Beyer**
  - Lockheed Martin Corporation
- **James Godwin**
  - BriteWerx, Inc
- **Jason Gorey**
  - Six O’Clock Ops
- **Michele Moss**
  - Booz Allen Hamilton
- **Fran Zenzen**
  - Arizona State Enterprise

### Manufacturing
- **Dean Bartles**
  - ASME
- **Larry John**
  - ANSER
- **Michael McGrath**
  - McGrath Analytics LLC
- **Catherine Ortiz**
  - Defined Business Solutions
- **Chris Peters**
  - The Lucrum Group
- **Tim Shinbara**
  - The Association for Manufacturing Technology
- **Devu Shila**
  - United Technologies Research Center
- **Joseph Spruill**
  - Lockheed Martin Corp
- **Rebecca Taylor**
  - Nat’l Center for Mfg. Sciences

### Logistics
- **Marilyn Gaska (Team Leader)**
  - Lockheed Martin Corp
- **Irv Varkonyi**
  - SCOPE

### Systems Engineering
- **Vicki Barbur**
  - MITRE
- **David Huggins**
  - Georgia Tech Research Institute
- **Thomas McCullough**
  - Lockheed Martin Corporation
- **Thomas McDermott**
  - Georgia Tech Research Institute
- **Heather Moyer (Team Leader)**
  - Consultant
- **Frank Serna**
  - Draper
- **Sarah Stern (Team Leader)**
  - Boeing
CFAM JWG is a Diverse Team

48 participants: Government, Academia, Industry, Associations and FFRDCs

• Government organizations:
  – DoD Undersecretary for Acquisition, Technology & Logistics
  – DoD Chief Information Officer
  – Department of the Army
  – Space and Naval Warfare Systems Command
  – Air Force Research Laboratory
  – Department of Energy
  – National Institute of Standards and Technology
  – Defense Microelectronics Activity
  – Manufacturing Technology ODASD (MIBP)
  – Defense Intelligence Agency
  – Idaho National Laboratory

• FFDRCs:
  – Institute for Defense Analyses
  – MITRE
  – Sandia National Laboratories

• Industry member organizations:
  – National Defense Industrial Association (lead)
  – American Society of Mechanical Engineers
  – Association for Enterprise Information
  – Association for Manufacturing Technology
  – National Center for Manufacturing Sciences

• Industry company representation:
  – ANSER
  – ARAR Technology
  – Boeing
  – Booz Allen Hamilton
  – Defined Business Solutions LLC
  – DRAPER
  – GLOBALFOUNDRIES
  – IPDE Systems, Inc.
  – Lockheed Martin
  – McGrath Analytics LLC
  – MTEQ
  – PricewaterhouseCoopers
  – Six O’Clock Ops
  – SCOPE
  – The Lucrum Group
  – United Technologies Research Center

• Academia:
  – Arizona State University Research Enterprise
  – Georgia Tech Research Institute
  – Wichita State University

November 15, 2016
The Digital Thread as DoD sees It

Requirements
- Research and Engineering Development
- Test and Evaluation
- Production

Product Lifecycle
- Training
- Sustainment
- Maintenance

Corporate Functions and Network
- Facilities
- Procurement
- Financial Programs
- Marketing
- R&D

Major Manufacturer
- Production Functions and Network

Production ICS OEM
- ICS Products and Services

Smaller Supplier (Cleared)
- Weak

Smaller Supplier (Uncleared)
- Weak

Production ICS OEM
- Weak

R&D Laboratory
- Weak

Cyber Defenses
- Perimeter
  - Strong
  - Medium
  - Weak
- Interior
  - Strong
  - Medium
  - Weak

Manufacturers' Production Functions and Network
- Level 2 (Monitoring/Supervising Production)
- Level 1 (Sensing/Manipulating Production)
- Level 0 (Production Process)
Level 0 (Production Process)
Level 1 (Sensing/Manipulating Production)
Level 2 (Monitoring/Supervising Production)
**Corporate Functions and Network**

- Facilities
- Inventory
- Procurement
- Personnel
- Financial
- Programs
- Marketing
- R&D

**Production ICS OEM**

- ICS Products and Services
- Corporate Functions and Network
- R&D Laboratory

**Major Manufacturer**

- Production Functions and Network
- Design, Production and Administrative Data

**Smaller Supplier**

- Production Functions and Network
- Product Test Data

**R&D Laboratory**

- Research Data

**Product Lifecycle**

- Requirements Analysis
- Research and Engineering Development
- Test and Evaluation
- Production
- Training
- Sustainment
- Maintenance

**Cyber Defenses**

<table>
<thead>
<tr>
<th>Cyber Defense</th>
<th>Perimeter</th>
<th>Interior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Major Manufacturer</td>
<td>Strong</td>
<td>Strong</td>
</tr>
<tr>
<td>Smaller Supplier (Cleared)</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Smaller Supplier (Uncleared)</td>
<td>Weak</td>
<td>Weak</td>
</tr>
<tr>
<td>Production ICS OEM</td>
<td>Weak</td>
<td>None</td>
</tr>
<tr>
<td>R&amp;D Laboratory</td>
<td>Weak</td>
<td>None</td>
</tr>
</tbody>
</table>

**Manufacturers’ Production Functions and Network**

- Level 0 (Production Process)
- Level 1 (Sensing/Manipulating Production)
- Level 2 (Monitoring/Supervising Production)
**Corporate Functions and Network**
- Facilities
- Inventory
- Procurement
- Personnel
- Financial
- Programs
- Marketing
- R&D

**Production ICS OEM**
- ICS Products and Services
- Corporate Functions and Network

**R&D Laboratory**
- Research Products
- Corporate Functions and Network

**Major Manufacturer**
- Production Functions and Network

**Smaller Supplier**
- Production Functions and Network

**Product Lifecycle**
- Requirements Analysis
- Research and Engineering Development
- Test and Evaluation
- Production
- Training
- Sustainment
- Maintenance

**DIGITAL THREAD**
- Research
- Products
- Maintenance

**Cyber Defenses**
- Perimeter
- Interior
- Major Manufacturer: Strong, Strong
- Smaller Supplier (Cleared): Medium, Medium
- Smaller Supplier (Uncleared): Weak, None
- Production ICS OEM: Weak, None
- R&D Laboratory: Weak, None

**Manufacturers’ Production Functions and Network**
- Level 0 (Production Process)
- Level 1 (Sensing/Manipulating Production)
- Level 2 (Monitoring/Supervising Production)

**Manufacturers’ Use Case Tracking**
- Design
- Production
- Administrative

**Integrity Use Case Attacks**
- A
- B
- C
- D
- E
- F

**Manufacturers’ Production Functions**
- Production Scheduling
- Production Control
- Material and Energy Control
- Quality Assurance
- Product Inventory Control
- Product Shipping Administration
- Maintenance Management
- R&D and Engineering
**Corporate Functions and Network**

- Facility
- Inventory
- Procurement
- Personnel
- Financial
- Programs
- Marketing
- R&D

**Product Lifecycle**

- Requirements Analysis
- Research and Engineering Development
- Test and Evaluation
- Production
- Training
- Sustainment
- Maintenance

<table>
<thead>
<tr>
<th>Cyber Defenses</th>
<th>Perimeter</th>
<th>Interior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Major Manufacturer</td>
<td>Strong</td>
<td>Strong</td>
</tr>
<tr>
<td>Smaller Supplier (Cleared)</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Smaller Supplier (Uncleared)</td>
<td>Weak</td>
<td>None</td>
</tr>
<tr>
<td>Production ICS OEM</td>
<td>Weak</td>
<td>None</td>
</tr>
<tr>
<td>R&amp;D Laboratory</td>
<td>Weak</td>
<td>None</td>
</tr>
</tbody>
</table>

**Digital Thread**

**Manufacturers’ Production Functions and Network**

- Level 2 (Monitoring/Supervising Production)
- Level 1 (Sensing/Manipulating Production)
- Level 0 (Production Process)
The Digital Thread is Vulnerable

Confidentiality
• Insiders can do recon and data exfiltration or alter design or process control files
• Insecure external/internal communications can be exploited to steal design data
• Sensors embedded in equipment can contain malware
• Visitors and contractors may have extensive or unsupervised access to software, firmware and hardware
• Tainted firmware from supply chain can contain sophisticated malware
• HVAC systems can be used to alter the process environment to damage/destroy products

Integrity
• Adversarial
• Accidental
• Structural
• Environmental

Availability
• Policy and Procedure
• Architecture and Design
• Configuration Management
• Physical
• Software Development
• Communication and Network

Large companies may be OK on their own, but what about the small and mid-size firms that may be connected to the big companies?

NIST 800-82 rev. 2

November 15, 2016
Small and Mid-Size Firms

- Often lack cybersecurity knowledge and resources. Most have no full time cybersecurity staff
  - ISA99 Standards and NIST SP 800-82 are complex. No turnkey solutions.
  - Forums available to large companies are often beyond their reach – e.g. DIB CS/IA Program requires facility clearance and COMSEC account
  - Cannot afford differing cybersecurity requirements from different customers

- Believe they are not targets, so they focus on perimeter defense for IT network
  - Lack of compartmentalization despite standards calling for discrete zones and conduits
  - Vulnerable to OEM backdoors, default passwords, discoverable IP addresses, connection by portable devices, connection from outside networks

May simply lack a business case for investing in OT cybersecurity
Status

- Each working group will present their findings and recommendations. 
  
  *... comments from today will be incorporated into final white paper.*

- Website will continued to be updated on NDIA portal. 
  
  *... found under Industrial Working Groups.*

- Outreach plan developed to share progress. 
  
  *... first public forum was in August, this second forum is to share findings; CFAM session at DMC on November 29th.*

- Goal is to brief senior OSD leadership in December 2016. 
  
  *... Formal report will be coordinated within DoD, and other government agencies as appropriate, after new leadership team is in place.*