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

*IT solutions do not fit Manufacturing Operations needs!*
Recommendations for USD(AT&L)

1. Designate a focal point to work with industry on risk-based, voluntary standards and practices for factory floor cybersecurity.
   - Evaluate NIST framework as starting point.

2. Conduct forums with industry to help understand and implement DFARS clause, including factory floor implications.
   - NDIA host factory floor discussion within AIA/Multi-association forum

3. Update DoD guidance on the Program Protection Plan (PPP) to address protection of manufacturing systems

4. Use red teams to expose vulnerabilities, sponsor R&D to fill gaps

5. Assist SME suppliers with training and investments. Explore:
   - NIST Manufacturing Extension Partnership to deliver training
   - Defense Prod Act Title III and Manufacturing Technology possibilities
   - Training for DoD contracting officers
Dialogue Initiated with DoD

NDIA Letter to USD(AT&L), May 2014

- Industry preference for voluntary framework
- 5 recommendations

USD(AT&L) Reply, July 2014

- Voluntary compliance insufficient
- “Let’s get together”
1. Designate a focal point to work with industry
2. Conduct forums with industry to help understand and implement DFARS clause, including factory floor implications.
3. Update DoD guidance on the Program Protection Plan (PPP).
4. Use red teams to expose vulnerabilities, sponsor R&D to fill gaps
5. Assist SME suppliers with training and investments

19 Dec 2014 – Meeting with Kristen Baldwin, ODUSD(SE): (Gen Bates and Mike McGrath from NDIA)

- Melinda Reed will be OSD interface coordinator
- NDIA will form new Joint Working Group to work with DoD on recommendations 2-5
  - Manufacturing, Cyber, SE and Logistics Divisions
Volunteers for the new JWG!

Need members and potential co-chair.

michael.mcgrath@anser.org
DMC 2014
Summary of the White Paper
Cyber Division & Manufacturing Division
Joint Working Group

Cyber Security for the Advanced Manufacturing Enterprise

Defense Manufacturing Conference
December 1, 2014

Michael McGrath
Consultant, Analytic Services Inc.
michael.mcgrath@anser.org
Advanced Manufacturing is:

- Driven by a “Digital Thread” of product and process information – valuable intellectual property (IP)
- Networked at every level to gain efficiency, speed and quality
- Targeted by global cyber threats

Common Visions
Smart Manufacturing, Industrial Internet, Industry 4.0, …
The Internet of Things!

Manufacturing is a Cyber-physical Business
The Threat is Global and Growing
Manufacturing is an inviting target

Manufacturing: a 1 in 3 chance of being targeted by at least one Spear Phishing attack in 2013

Symantec Internet Security Report 2014

Cost to Global Economy > $400 B
Part of the Internet of Things (IoT)

Smart Processes, Smart Products

IoT Bi-directional Relationship with Manufacturing

“SMART MANUFACTURING”

IoT technologies optimize manufacturing processes (automation, tracing, tracking, etc.) and human-enterprise interaction

Revenue

“IoT-embedded” manufactured products transform the socio-economic fabric (marketing, sales, information management, business models, service industry, etc.)

“MANUFACTURING SMART”

Cost

Source: Alain Louchez, Georgia Tech Center for Development and Application of IoT Technologies
www.cdait.gatech.edu
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!

www.ndia.org/Divisions/Divisions/Manufacturing
Scope: Protecting the Digital Thread
Technical Data in the Advanced Manufacturing Enterprise

Targeted by nation states, terrorists, criminals and hacktivists.

IT Cyber Security Solutions May Not Fit Manufacturing Operations Needs
What We Heard from Interviews

Gov’t, Industry, Academia

- CIOs/CISOs in the defense primes are implementing strong cyber risk management and sharing info through the DIB CS/IA and DSIE programs
  - Concerned about suppliers and willing to work with them
  - Have not yet seen threat to factory systems, but acknowledge the possibility
  - Need cost/risk tradeoffs to arrive at an affordable solution

- Industrial Control Systems (ICS) are soft targets. Culture differs from IT.
  - Standards and guides* for ICS provide good risk management approaches. Implementation is spotty.

- DoD has mandated protection of critical information
  - Primes address in the program protection plan, but ICS security is not emphasized in DoD guidance

- Defense R&D for cybersecurity is not currently focused on factory floor

*E.g. ANSI/ISA99 standards and NIST SP 800-82
2014 Developments

Federal Register 18 Nov 2013 -- DFAR 252.204–7012 Safeguarding of unclassified controlled technical information.

- Specifies 54 minimum security controls linked to NIST SP 800-53
- Reporting of cyber incidents to DoD within 72 hours
- Reviews and data retention to support DoD Damage Assessments
- Mandatory flow-down to subcontracts

NIST Cybersecurity Framework for Critical Infrastructure Protection (Feb 2014)

- Common vocabulary, core standards and practices
- Risk-based. Voluntary adoption.
- Sector-specific implementation, including training and incentives.
2014 Developments (2 of 2)

  - Updates threats and vulnerabilities, risk management, recommended practices, security architectures, and security capabilities and tools for Industrial Control Systems.

- NSTAC Report to the President on Internet of Things (Draft Nov 2014)

- NDIA White Paper to USD(AT&L) (May 2014, discussions ongoing)
  - Industry preference for voluntary framework
  - 5 recommendations
1. Designate a focal point to work with industry on risk-based, voluntary standards and practices for factory floor cybersecurity.
   - Evaluate NIST framework as starting point.
2. Conduct forums with industry to help understand and implement DFARS clause, including factory floor implications.
3. Update DoD guidance on the Program Protection Plan (PPP). Let industry make appropriate risk/cost tradeoffs.
4. Use red teams to expose vulnerabilities, sponsor R&D to fill gaps.
5. Assist SME suppliers with training and investments
   - NIST Manufacturing Extension Partnership to deliver training
   - Defense Prod Act Title III and Manufacturing Technology investments
   - Training for DoD contracting officers