Cybersecurity for Advanced Manufacturing (CFAM)

An NDIA Joint Working Group

Manufacturing Readiness Level Working Group

April 24, 2018

Talk Outline

- Manufacturing Today
- NDIA Joint Working Group Study
- Relevancy to MRL Criteria

Today's Manufacturing Environment

Manufacturing is an increasingly digital business

Smart Manufacturing

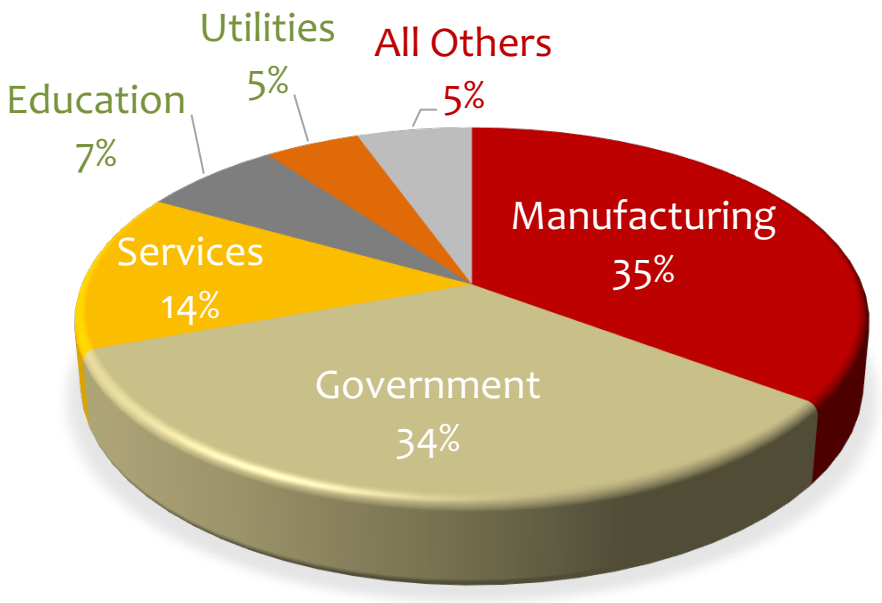
Industrial Internet of Things

Industry 4.0

- 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

Cybersecurity: Manufacturing is Under Attack

Percent of 2016 Cyber Espionage Incidents, by Industry



Source: 2017 Verizon Data Breach Investigations Report

- Over half of companies operating industrial control systems (ICS) worldwide suffered between one and five IT security incidents in the last year
- 81% of companies report increased use of wireless connections to the industrial network
- 54% haven't implemented vulnerability scanning and patch management
- Half allow external providers to have access to their industrial control networks

Source: Kaspersky Labs, State of Industrial Cybersecurity 2017 Survey

Operational Technology

ICS systems are long-lived capital investments (15-20 year life)

"Production mindset" with little tolerance for OT down time

Nascent cybersecurity awareness and limited workforce training

Manufacturing production processes bring executable code into system

Technical data flowing through the system is highly valued by adversaries

These are Not Cooperative R&D Efforts


U.S. Reaper


China's Yìlóng-1


U.S. HUMVEE

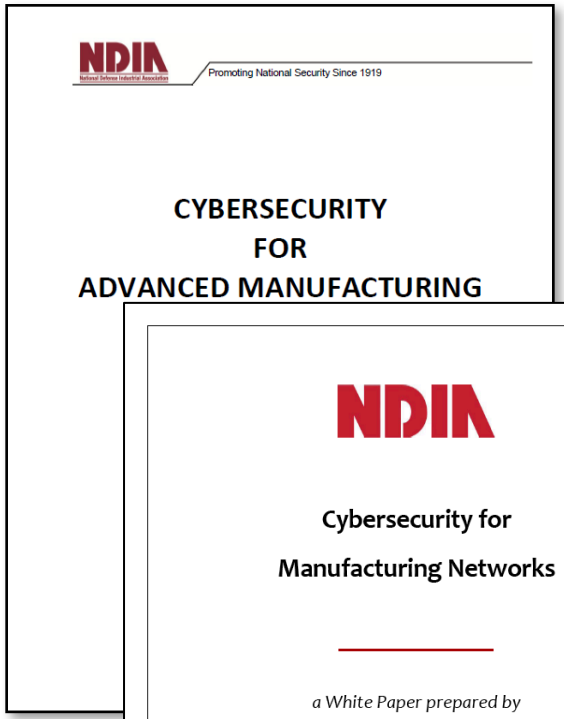

China's Dongfeng EQ2050

Credit to Brian Hughes, Director of the Office of the Secretary of Defense (OSD) Damage Assessment Management Office (DAMO)

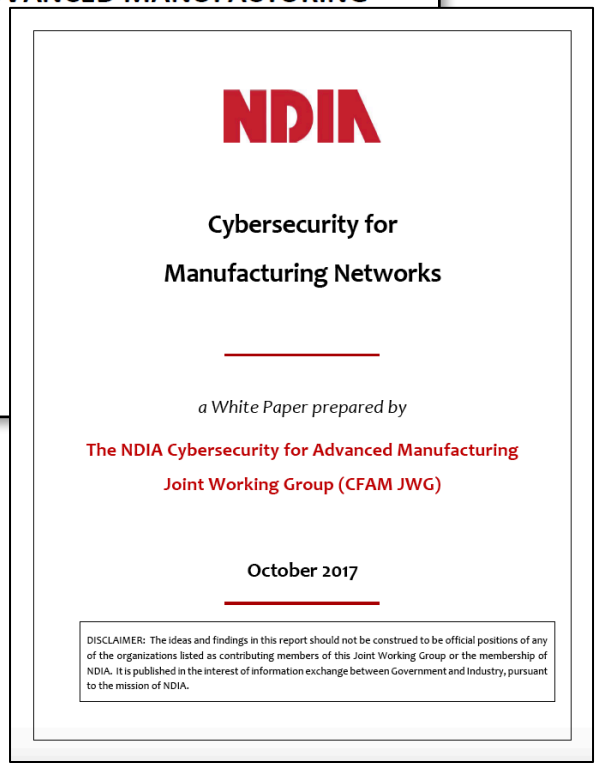
NDIA Study Elements

NDIA White Papers: National Security Implications

2014



2017



Cyber risks in defense industrial base are national security concerns

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

http://www.ndia.org/divisions/working-groups/cfam/resources

The Attack Scenarios Are Real

Product tampering

TechRepublic.

3D printing hack: Researchers crash drone with sabotaged propeller

Researchers from three universities recently completed an attack on a 3D additive manufacturing system, highlighting the impact of potential security vulnerabilities in such systems.

By Conner Forrest | October 20, 2016, 6:00 AM PST

University researchers were able to sabotage a drone by hacking the computer controlling the 3D printer that made its parts, according to a research paper released Thursday. By changing the design of the propellor before printing, they caused the $1,000 drone to "smash into the ground" and break, shortly after take off.

REUTERS

INNOVATION AND INTELLECTUAL PROPERTY | Thu Dec 8, 2016 | 11:53am EST

ThyssenKrupp secrets stolen in 'massive' cyber attack

By **Eric Auchard** and **Tom Käckenhoff** | FRANKFURT

Technical trade secrets were stolen from the steel production and manufacturing plant design divisions of ThyssenKrupp AG (TKAG.DE) in cyber attacks earlier this year, the German company said on Thursday.

ThyssenKrupp, one of the world's largest steel makers, said it had been targeted by attackers located in southeast Asia engaged in what it said were "organized, highly professional hacker activities".

Intellectual property theft

Physical damage

BBC Sign in | News | Sport | Weather | Shop | Earth | Travel | More

NEWS

Hack attack causes 'massive damage' at steel works

22 December 2014 | Technology

Share

The hack attack led to failures in plant equipment and forced the fast shut down of a furnace

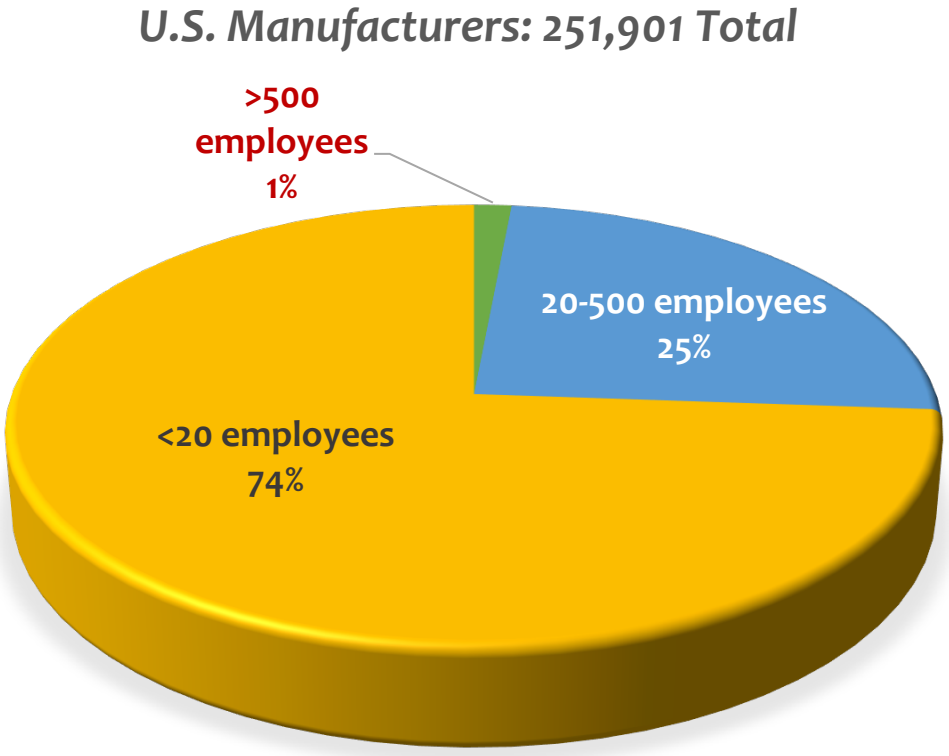
A blast furnace at a German steel mill suffered "massive damage" following a cyber attack on the plant's network, says a report.

NDIA CFAM JWG was a Diverse Team

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

- **Government organizations:**
  - DoD Undersecretary for Acquisition, Technology & Logistics
  - Joint Chiefs of Staff
  - DoD Chief Information Officer
  - Department of the Army
  - Space and Naval Warfare Systems Command
  - Air Force Research Laboratory
  - Department of Energy
  - White House Office of Science and Technology Policy
  - National Institute of Standards and Technology
  - Academia:
  - Arizona State University
  - Georgia Tech Research Institute
  - Wichita State University
- **Industry company representation:**
  - ANSER
  - Boeing
  - Booz Allen Hamilton
  - DRAPER
  - GLOBALFOUNDRIES
  - Lockheed Martin
  - PricewaterhouseCoopers
  - United Technologies Research Center
  - Other small companies and consultancies
- **Industry member organizations:**
  - Association for Manufacturing Technology
  - Digital Manufacturing and Design Innovation Institute
  - National Center for Manufacturing Sciences
- **FFDRCs:**
  - Institute for Defense Analyses
  - Sandia National Laboratories

Cybersecurity: Most Manufacturers are Small & Medium Enterprises (S&MEs)



Source: http://www.nam.org/Newsroom/Facts-About-Manufacturing/20170615

- Often lack cybersecurity knowledge and resources
- Most have no full time cybersecurity staff
- Believe they are not targets, so they focus on perimeter defense for IT network
- Many lack a business case for investing in OT cybersecurity

S&MEs are critical to manufacturing sector and are most vulnerable

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

Product Lifecycle

DIGITAL THREAD

Corporate Functions and Network

Facilities Inventory
Procurement Personnel
Financial Programs
Marketing R&D

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

Major Manufacturer

Production Functions and Network

1 2 3 4 5 6

Corporate Functions and Network

Production ICS OEM

ICS Products and Services

Corporate Functions and Network

Maintenance Data

Performance Data

Maintenance Data

Performance Data

Design, Production and Administrative Data

1	Product Data
2	Process Data
3	Production Status
4	Process Performance
5	Product Status
6	Product Test Data

Research Data

Research Data

Research Products

Corporate Functions and Network

R&D Laboratory

Production Functions and Network

1 2 3 4 5 6

Corporate Functions and Network

Smaller Supplier

Manufacturers' Production Functions and Network

Level 2 (Monitoring/Supervising Production)

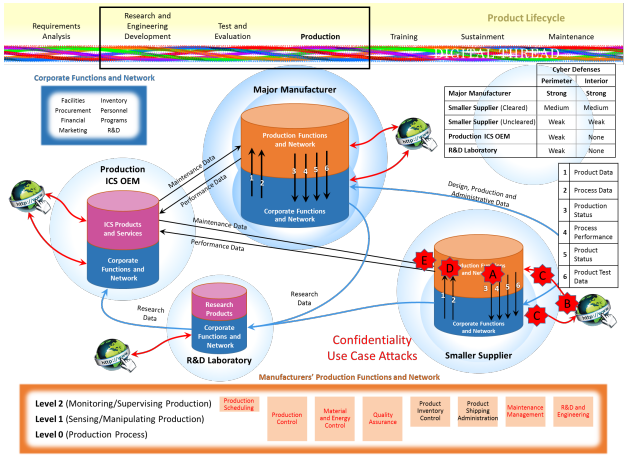
Level 1 (Sensing/Manipulating Production)

Level 0 (Production Process)

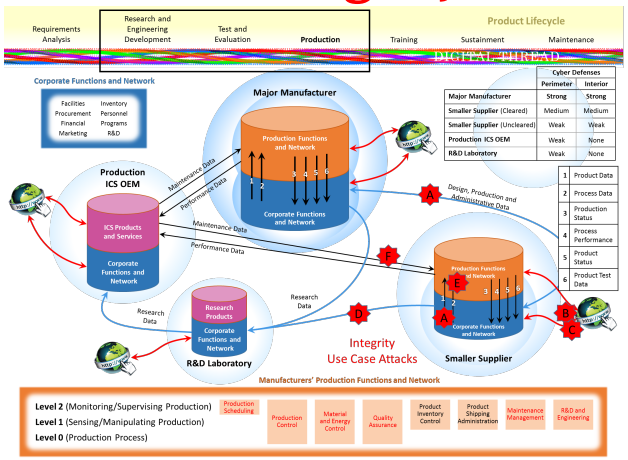
Production Scheduling | Production Control | Material and Energy Control | Quality Assurance | Product Inventory Control | Product Shipping Administration | Maintenance Management | R&D and Engineering

The Digital Thread is Vulnerable

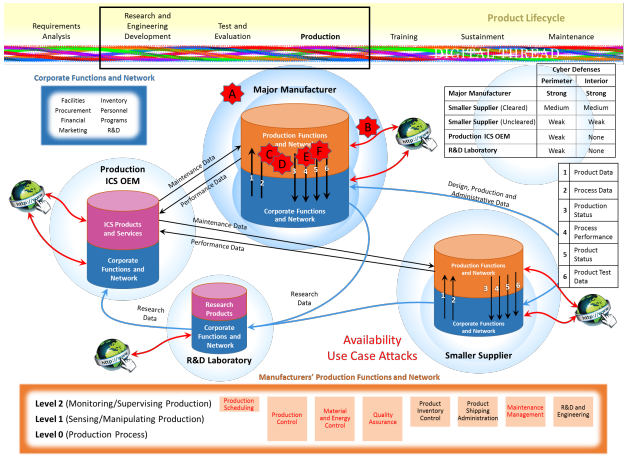
Confidentiality



Integrity



Availability



- 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

<u>Threat Types</u>

- Adversarial
- Accidental
- Structural
- Environmental

<u>Vulnerability Types</u>

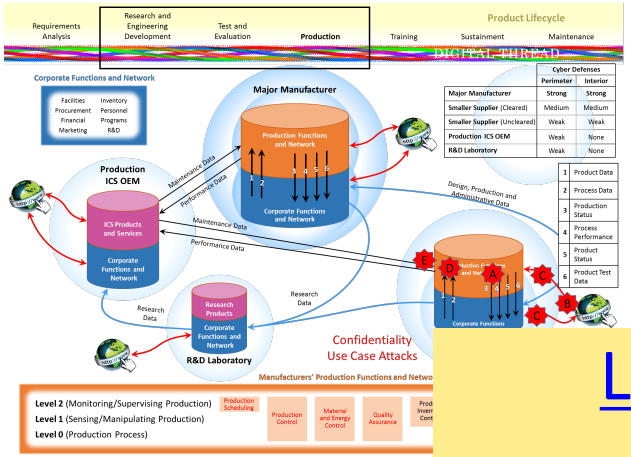
- Policy and Procedure
- Architecture and Design
- Configuration Management
- Physical
- Software Development
- Communication and Network

NIST 800-82 rev. 2

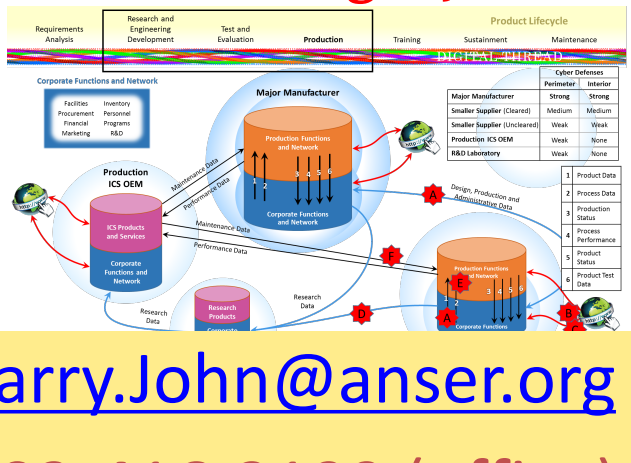
Large companies may be OK on their own, <u>but</u>
what about the small and mid-size firms that may be connected to the big companies?

The Digital Thread is Vulnerable

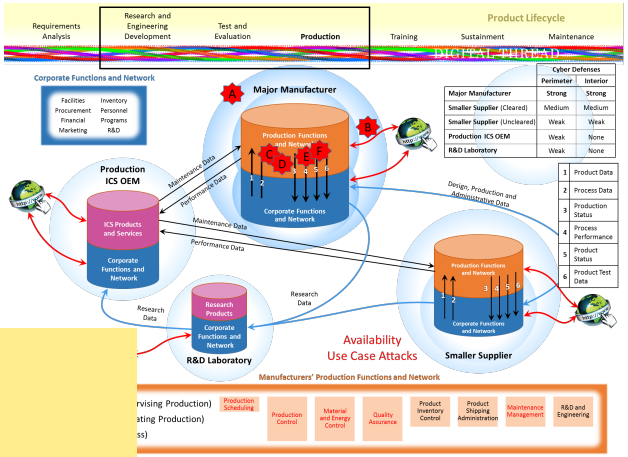
Confidentiality



Integrity



Availability



Larry.John@anser.org

703-416-3199 (office)

703-785-6331 (mobile)

- Insiders can do recon and process control files
- Insecure external/interna to steal design data
- Sensors embedded in equ
- Visitors and contractors r 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

NIST 800-82 rev. 2

- Architecture and Design
- Configuration Management
- Physical
- Software Development
- Communication and Network

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

NDIA CFAM JWG Vision

DoD and defense prime contractors are catalysts for creating a robust cyber-resilient U.S. industrial base connected through trustworthy manufacturing networks that respond rapidly to national security needs.

Summary of Findings

- The CFAM JWG identified six activities to address the manufacturing cybersecurity challenge, discussed below. These activities establish the foundation upon which the subsequent recommendations were formed.
  - ***Raise awareness*** of the manufacturing cybersecurity threats
  - ***Provide training*** at all organizational levels
  - ***Aggregate manufacturing cybersecurity activities*** that exist, or are being created, across the Federal government to raise visibility, consolidate resources, and improve the pace of progress
  - ***Enable collaboration*** among, and within, organizations working to better secure both OT and IT in manufacturers' operations.
  - ***Provide incentives*** to manufacturers to upgrade facilities that will improve cybersecurity while enhancing productivity, and to equipment providers to improve security in their products
  - ***Develop technology*** along two paths: immediately deployable improvements and long-term comprehensive solutions. Specifically, DoD could create or add to existing government-sponsored research programs designed to discover vulnerabilities within existing and emerging manufacturing networks

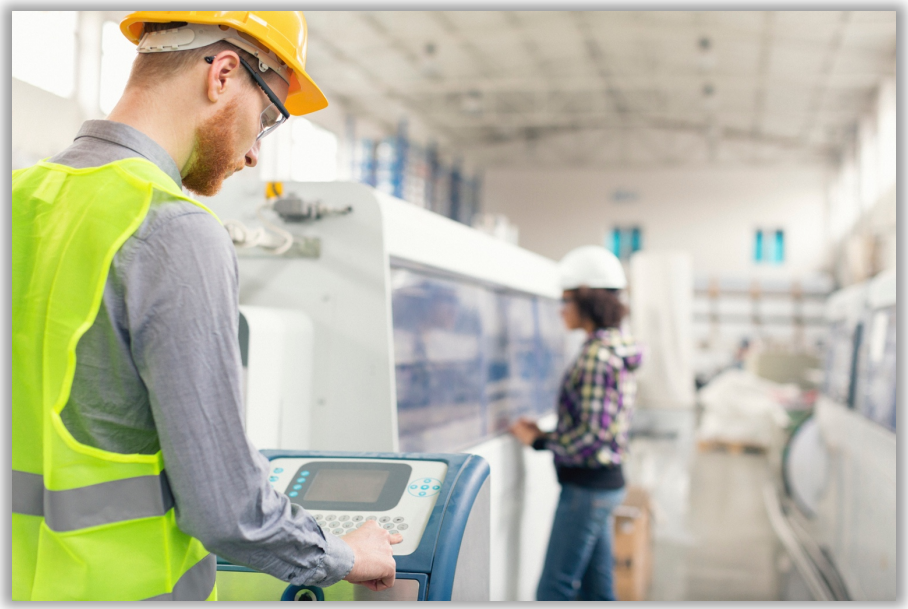
Top Level Recommendations

- Establish, and adequately fund, a new program for manufacturing cybersecurity capabilities in the industrial base, with a DASD-level champion
- Establish, and share the cost of, a Public-Private Partnership for Security in American Manufacturing
- Incentivize industrial modernization for cyber-secure defense manufacturing through the use of innovative contracting authorities
- Give high priority to R&D in cybersecurity for manufacturing through targeted project funding

Comprehensive approach is required . . . And should be launched without delay

DFARS: Small and Mid-Size Enterprises (S&MEs)

- Protecting controlled defense information (CDI) is greatest challenge for S&MEs – giving our adversaries soft entry points
- New DFARS require all contractors to protect information and the networks . . .
- But for SM&Es, these new regulations are largely unfunded mandates that impact their competitiveness



Absent incentives to assist DFARS and NIST implementation, DoD may find that fewer companies will be eligible suppliers for defense systems

Summary

- Combining ***manufacturing innovation*** and ***secure technological superiority*** will enable the U.S. to remain the world's dominant military power
  - Advanced manufacturing technology drives national economic performance, making it a ***critical enabler in fielding advanced technology weapon systems***
  - The benefits companies are gaining by adopting smart manufacturing technology are ***fueling a quick, permanent transition to the Fourth Industrial Revolution*** (Industry 4.0)
  - This revolution, however, ***opens gaping holes in security systems***, ***expands the attack surface, increases vulnerability of the manufacturing supply base***, and ***creates serious threats to national security***
- Implementing the CFAM JWG recommendations will deliver high value for the warfighters and taxpayers
  - Creating high-impact collaborations will ***strengthen the nation's technology value chain***, benefitting not only DoD but also the prime contractors who supply much of the materiel required for the nation's fighting forces ***and the small businesses that offer valuable innovation*** and are a source of much of the nation's economic growth
- The nation will benefit significantly by investing proactively in ***building a more secure DoD manufacturing infrastructure,*** creating a smarter defense against malicious actors, and allowing the U.S., and particularly the Defense Industrial Base, to stay ahead of the cyber-threat throughout the supply chain

MRL Criteria Relevancy

- Preliminary review of Al's MRL 1-4 Proposed Matrix suggests three areas with CFAM relevancy:
  - A.1 Industrial Base
    - How are CFAM threats addressed in the Industrial Base?
    - How do the systems integrators' contractual obligations transfer to lower tier suppliers?
  - A.2 Manufacturing Technology Development
    - How can cybersecurity be improved with technology?
    - How does new technology negatively impact cybersecurity?
  - H.2 Facilities
    - What cybersecurity protections can be implemented at the facility level?
    - Where are facility connections that degrade cybersecurity?

For more information:

Catherine Ortiz

cjortiz@definedbusiness.com

804-462-0564

Download the white papers:

http://www.ndia.org/divisions/working-groups/cfam/resources