NDIA and DoD Joint Working Group

Systems Approach for Cybersecurity for Advanced Manufacturing

"Protecting the Digital Thread"

NDIA Systems Engineering Conference
Springfield, VA
October 19th, 2016

Dr. Marilyn Gaska, Lockheed Martin
Corporate Engineering, Technology, and Operations
Catherine Ortiz, Defined Business Solutions, LLC

Systems Approach for Cybersecurity for Advanced Manufacturing (CFAM)

Systems Approach for Cybersecurity for Advanced Manufacturing
Dr. Marilyn T. Gaska* and Ms. Catherine Ortiz**
***Lockheed Martin Corporate Engineering, Technology, and Operations**
**** Defined Business Solutions, L.L.C.**

Abstract (18943)
Introduction of any new advanced technology in a digital world can increase security risks. Advanced manufacturing, with reliance on digital information and industrial control systems (ICS), can introduce capabilities and reduce lifecycle costs, but it can also increase security risk for both manufacturing and sustainment. In 2014 the Joint Working Group on Cybersecurity for Advanced Manufacturing (CFAM) published an initial white paper on this topic. Both the National Defense Industrial Association (NDIA) Manufacturing and Cyber Divisions were engaged. With support of Office of the Secretary of Defense (OSD) Under Secretary of Defense for Acquisition, Technology & Logistics (AT&L) Mr. Frank Kendall, a subsequent Joint Working Group has focused on implementation plans and expanded involvement to include OSD Systems Engineering sponsor with NDIA Systems Engineering, Cyber, Manufacturing, and Logistics Division engagement. Membership includes key participants from other related cyber initiatives in the Digital Manufacturing and Design Innovation Institute (DMDII) and the National Institute of Standards and Technology (NIST). This presentation will highlight the application a systems approach to analyzing the cybersecurity in advanced manufacturing risks and developing mitigation recommendations. This includes stakeholder agreement of scope and common definitions (terms of reference) by an overall Integration Team for use by the Policy, Planning, and Impacts Team, the Manufacturing Environment Team, and the Technology Solutions Team. The scope was mapped to the American National Standards Institute (ANSI) International Society of Automation (ISA) 95.00.01 to show the manufacturing environment functional process and supporting data flow diagrams. Three use cases for confidentiality, availability, and integrity were developed to assist technology solution development. Subject Matter Expert (SME) interviews were conducted as part of the requirements definition and existing resource identification process. The holistic approach has also addressed education and culture change management for organizations of all sizes. The presentation will provide an opportunity for peer feedback prior to finalization of the recommendations in December 2016.

Agenda

- Context and CFAM Joint Working Group History
- Systems and Team Approach
- Stakeholder / Standards-Based Scope and Definitions
- Systems Approach Utilizing Use Cases and Interviews
- Holistic Approach from Risks to Culture Change

Manufacturing is a Cyber-physical Business

Common Visions

Smart Manufacturing,

Industrial Internet,

Industry 4.0, …

The Internet of Things!

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

Why This is Important

These are Not Cooperative R&D Efforts

From Brian Hughes' presentation at 2015 NDIA Systems Engineering Conference

U.S. Reaper

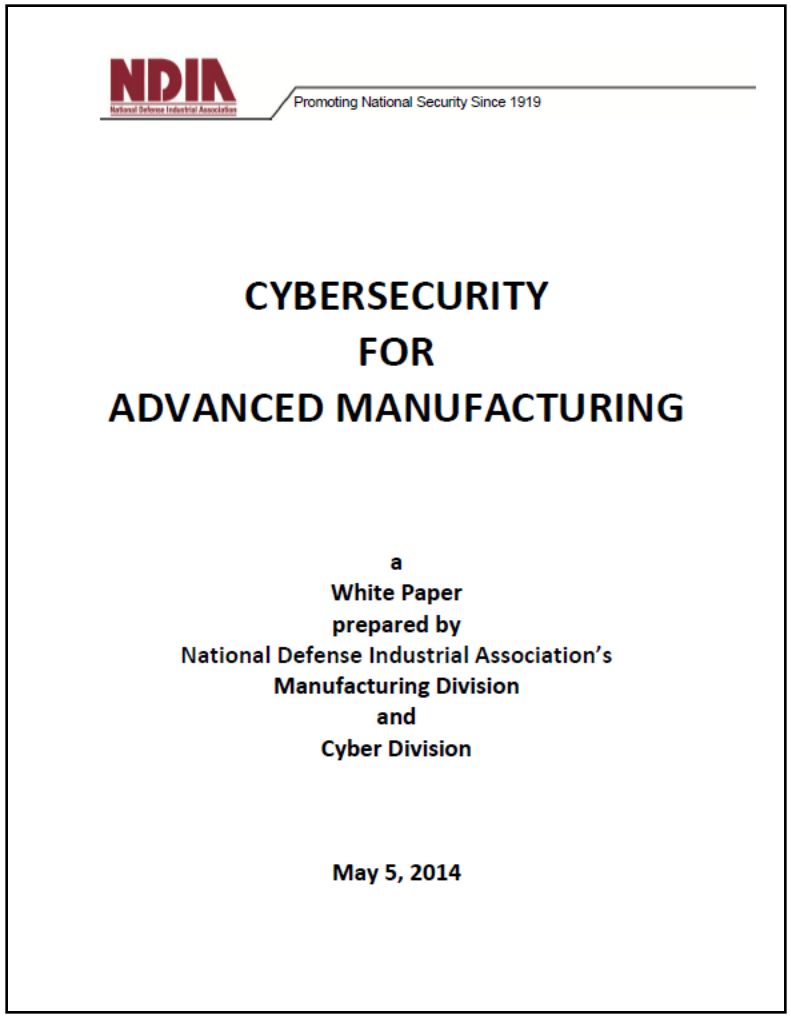
China's Yìlóng-1

U.S. HUMVEE

China's Dongfeng EQ2050

NDIA White Paper

Protecting the Digital Thread



NDIA
National Defense Industrial Association
Promoting National Security Since 1919

CYBERSECURITY
FOR
ADVANCED MANUFACTURING

a
White Paper
prepared by
National Defense Industrial Association's
Manufacturing Division
and
Cyber Division

May 5, 2014

www.ndia.org/Divisions/Divisions/Manufacturing

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***

Systems Approach

- **48 participants: 13 Government, 9 from membership or academic organizations, 24 company representatives and 2 FFRDCs**
- **Engaging discussion between Government and NDIA participants . . .** ***current situation, desired outcomes, barriers, opportunities***
- **Teams formed to work on problem areas**
  - Policy Planning and Impacts Team
  - Technology Solutions Team
  - Manufacturing Environment Team
- **Supported by Integration Team to ensure limited overlap and to resolve conflicts**

Preliminary Questions to be Addressed

- **Boundaries . . .**
  - What defines a manufacturing environment?
  - What use cases are important across the life cycle of the manufacturing environment?
- **Mitigations . . .**
  - What actions and activities can improve cybersecurity in the manufacturing environment?
  - What types of education, training and cultural changes are required?
- **Development . . .**
  - What technical solutions can increase cybersecurity in the manufacturing environment?
- **Resources . . .**
  - What existing policies regulations, and standards are applicable and what needs to be augmented, and by whom?
  - What activities implemented outside the Department of Defense can be leveraged?

Integration Team

- **This group will create the charter and scope of the CFAM JWG, and will support other teams as needed.**
- **Team Lead: Catherine Ortiz, Defined Business Solutions**

Robert Badgett IPDE Systems, LLC	**James Godwin** PricewaterhouseCoopers	**Michele Moss** Contract support to DOD Office of CIO	**James Poplin** Defined Business Solutions
Vicki Barbur Consultant	**Larry John** ANSER	**Catherine Ortiz** Defined Business Solutions	**Melinda Reed** ODASD(SE)
Dawn Beyer Lockheed Martin Corporation	**Michael McGrath** McGrath Analytics LLC	**Chris Peters** The Lucrum Group	**Stephanie Shankles** Contract support to DOD Office of CIO
Donald Davidson Office of the DoD CIO			**Joe Spruill** Lockheed Martin Corporation

Manufacturing Environment Team

- **This group will identify actions and activities that can have the greatest impact to improve cybersecurity in the manufacturing environment, and will recommend implementation processes**
- **Team Lead: Dr. Marilyn Gaska, Lockheed Martin Corporation**

Sean Atkinson Global Foundries	**Dan Green** SPAWAR	**Sean Miles** Defense Intelligence Agency	**Rebecca Taylor** Nat'l Center for Mfg. Sciences
Dean Bartles	**Daryl Haegley** OASD (EI&E) IE	**Chris Peters** The Lucrum Group	**Irv Varkonyi** SCOPE
Michael Dunn ANSER	**Larry John** ANSER	**Adele Ratcliff** AT&L MIBP	**Mary Williams** MTEQ
Aman Gahoonia DMEA	**Greg Larsen** Institute for Defense Analyses	**Haley Stevens / Andrew Watkins** DMDII	**Fran Zenzen** Arizona State University Research Enterprise
Marilyn Gaska Lockheed Martin Corporation	**Thomas McCullough**	**Keith Stouffer** NIST	**+Integration Team Reps**

Technology Solutions Team

- **This team will establish an initial baseline of available and emerging technology solutions to improve cybersecurity in the DIB and deliver a Recommendations Report suggesting additional technology-based concepts that should be explored.**
- **Team Lead: Heather Moyer, Consultant**

Robert Badgett Consultant	**Anitha Raj** ARAR Technology	**Devu Shila** United Technologies Research Center
Vicki Barbur Consultant	**Craig Rieger** Idaho National Laboratory	**Tim Shinbara** The Association for Manufacturing Technology
Heather Moyer Consultant	**Frank Serna** DRAPER	**Janet Twomey** Wichita State University

Policy Planning & Impacts Team

- **This team will 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.**
- **Team Lead: Sarah Stern, Boeing BCA Network Cyber Security**

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	**Bill Trautmann** JSJ4, KBLD
Jason Gorey Six O'Clock Ops	**Michele Moss** Contract support to DOD Office of CIO	**Sarah Stern** Boeing, BCA Network Cyber Security	**Melinda Woods** AT&L MIBP

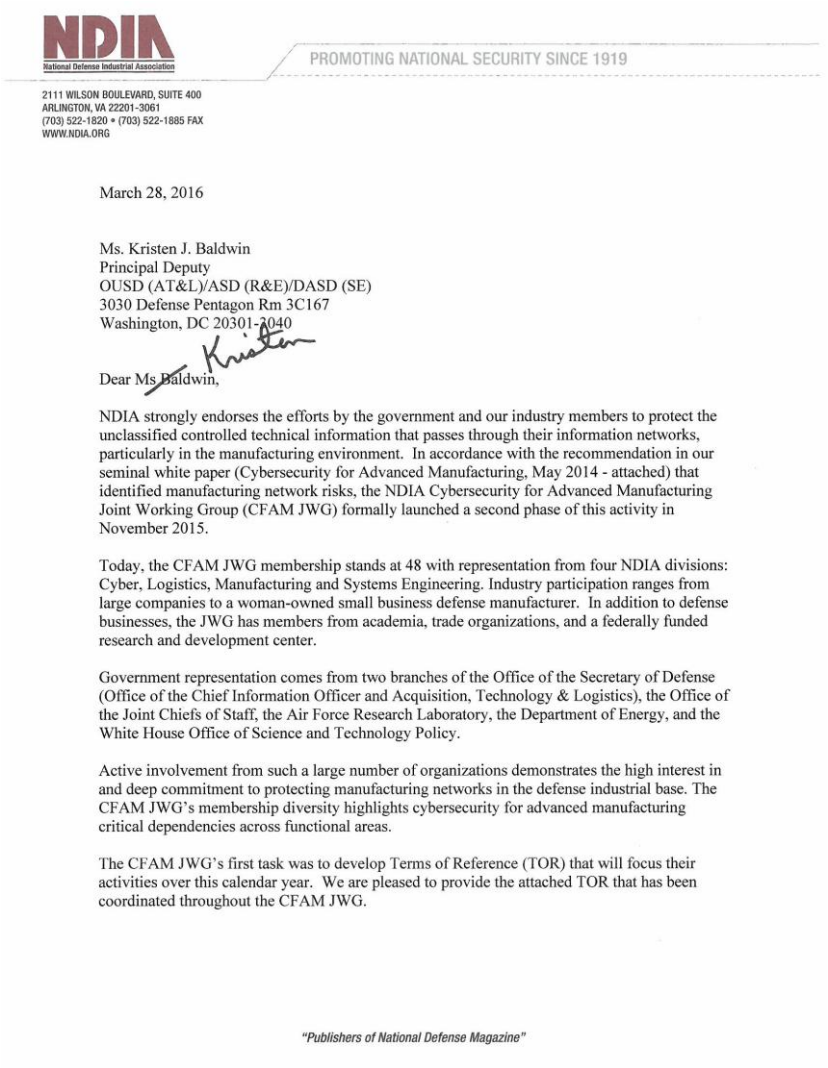
Scope: Protecting the Digital Thread

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.

Terms Of Reference



NDIA
National Defense Industrial Association

PROMOTING NATIONAL SECURITY SINCE 1919

2111 WILSON BOULEVARD, SUITE 400
ARLINGTON, VA 22201-3061
(703) 522-1820 • (703) 522-1885 FAX
WWW.NDIA.ORG

March 28, 2016

Ms. Kristen J. Baldwin
Principal Deputy
OUSD (AT&L)/ASD (R&E)/DASD (SE)
3030 Defense Pentagon Rm 3C167
Washington, DC 20301-3040

Dear Ms Baldwin,

NDIA strongly endorses the efforts by the government and our industry members to protect the unclassified controlled technical information that passes through their information networks, particularly in the manufacturing environment. In accordance with the recommendation in our seminal white paper (Cybersecurity for Advanced Manufacturing, May 2014 - attached) that identified manufacturing network risks, the NDIA Cybersecurity for Advanced Manufacturing Joint Working Group (CFAM JWG) formally launched a second phase of this activity in November 2015.

Today, the CFAM JWG membership stands at 48 with representation from four NDIA divisions: Cyber, Logistics, Manufacturing and Systems Engineering. Industry participation ranges from large companies to a woman-owned small business defense manufacturer. In addition to defense businesses, the JWG has members from academia, trade organizations, and a federally funded research and development center.

Government representation comes from two branches of the Office of the Secretary of Defense (Office of the Chief Information Officer and Acquisition, Technology & Logistics), the Office of the Joint Chiefs of Staff, the Air Force Research Laboratory, the Department of Energy, and the White House Office of Science and Technology Policy.

Active involvement from such a large number of organizations demonstrates the high interest in and deep commitment to protecting manufacturing networks in the defense industrial base. The CFAM JWG's membership diversity highlights cybersecurity for advanced manufacturing critical dependencies across functional areas.

The CFAM JWG's first task was to develop Terms of Reference (TOR) that will focus their activities over this calendar year. We are pleased to provide the attached TOR that has been coordinated throughout the CFAM JWG.

"Publishers of National Defense Magazine"

TOR was sent to:
Ms. Kristen Baldwin
OUSD (AT&L) ASD (R&E)/DASD (SE)

Signed by:
Craig R. McKinley
General, USAF (Ret)
President and CEO NDIA

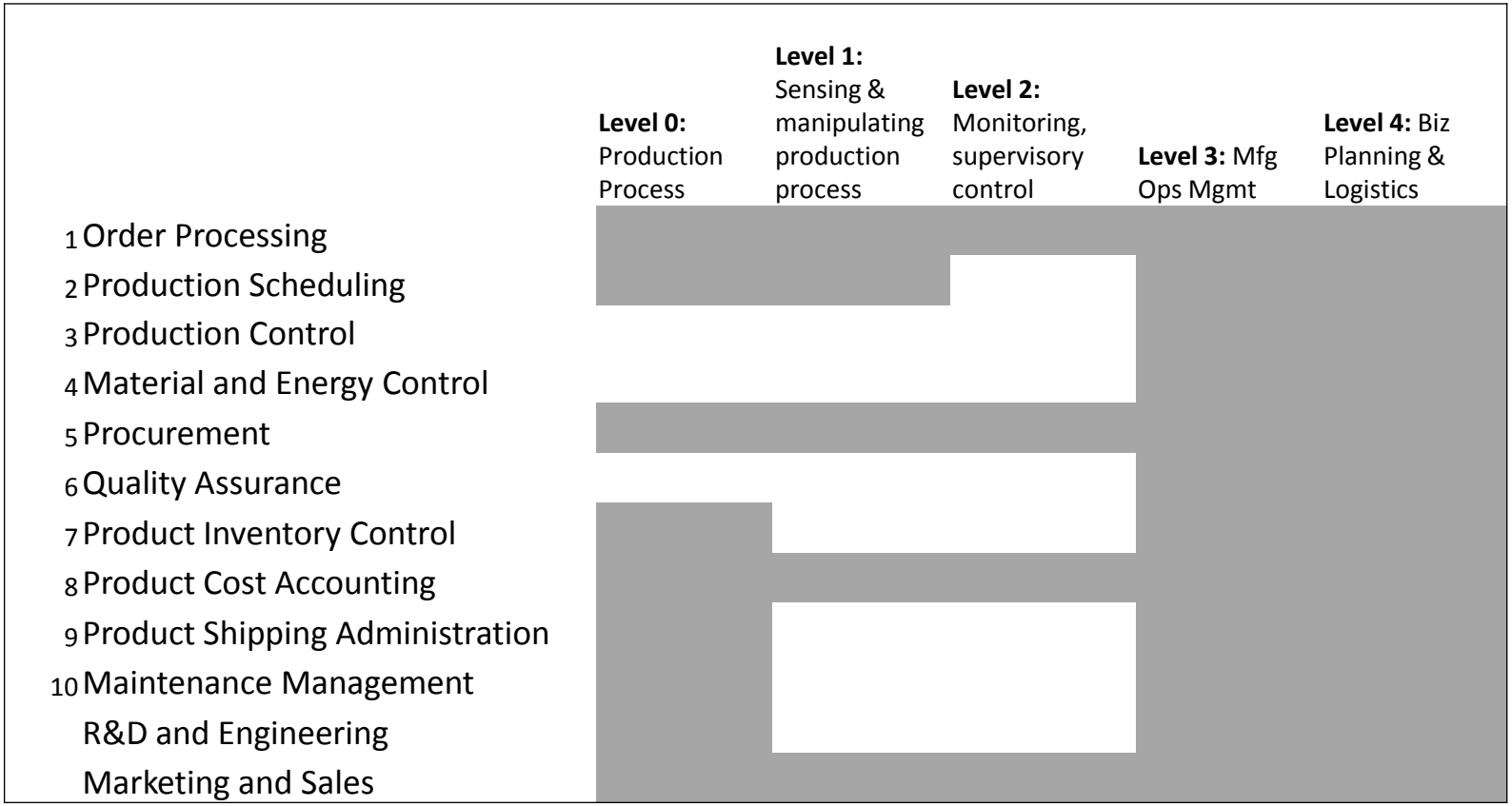
Copied were:
Aaron Hughes
DASD Cyber Policy USD(P)
And
Richard Hale
Deputy DoD-CIO for Cybersecurity

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
  - Weak privilege management among operators and maintainers. Growing use of wireless devices.
  - 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

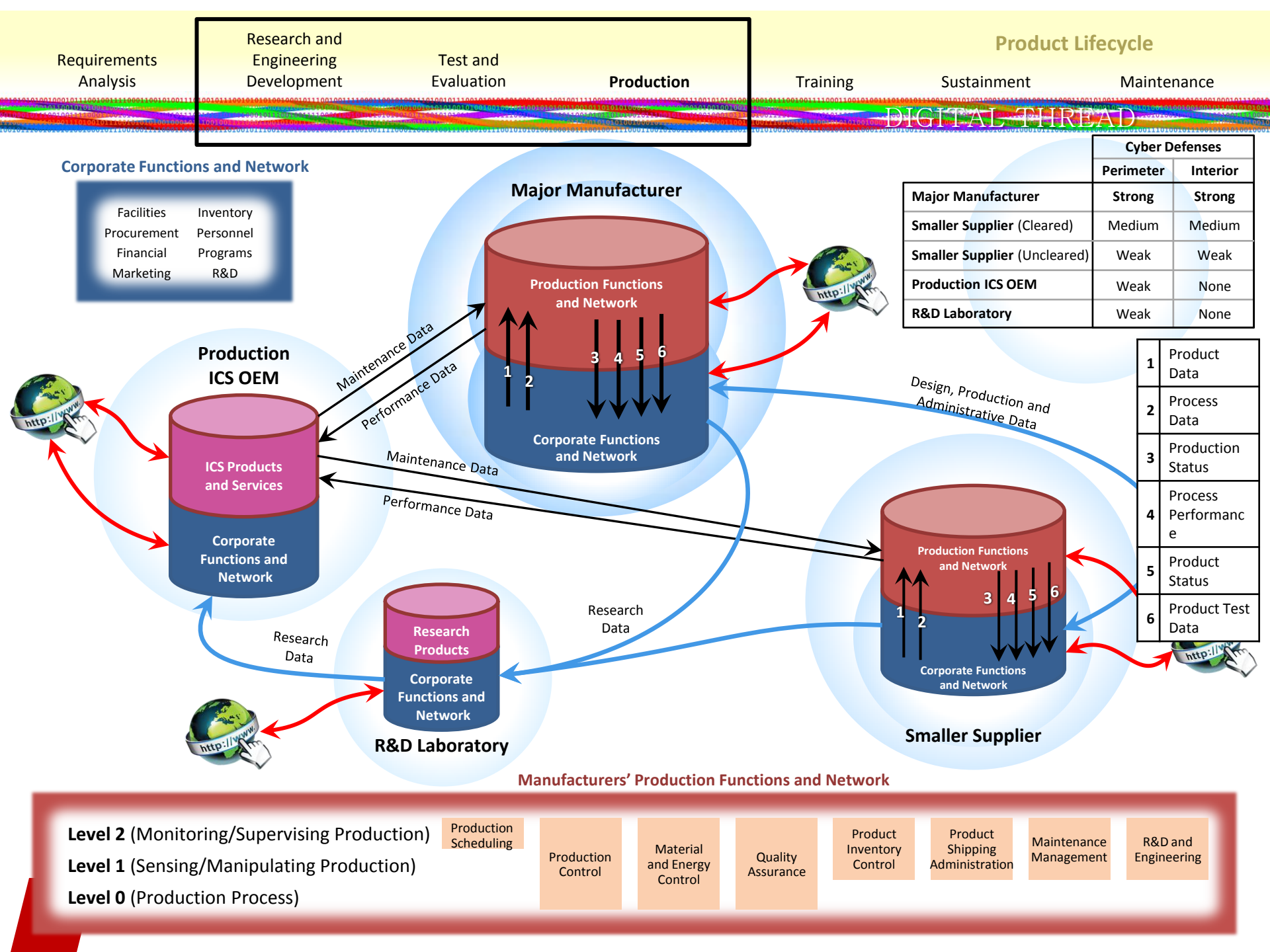
Standards Based Scope / Definitions: Manufacturing Environment Framework Matrix

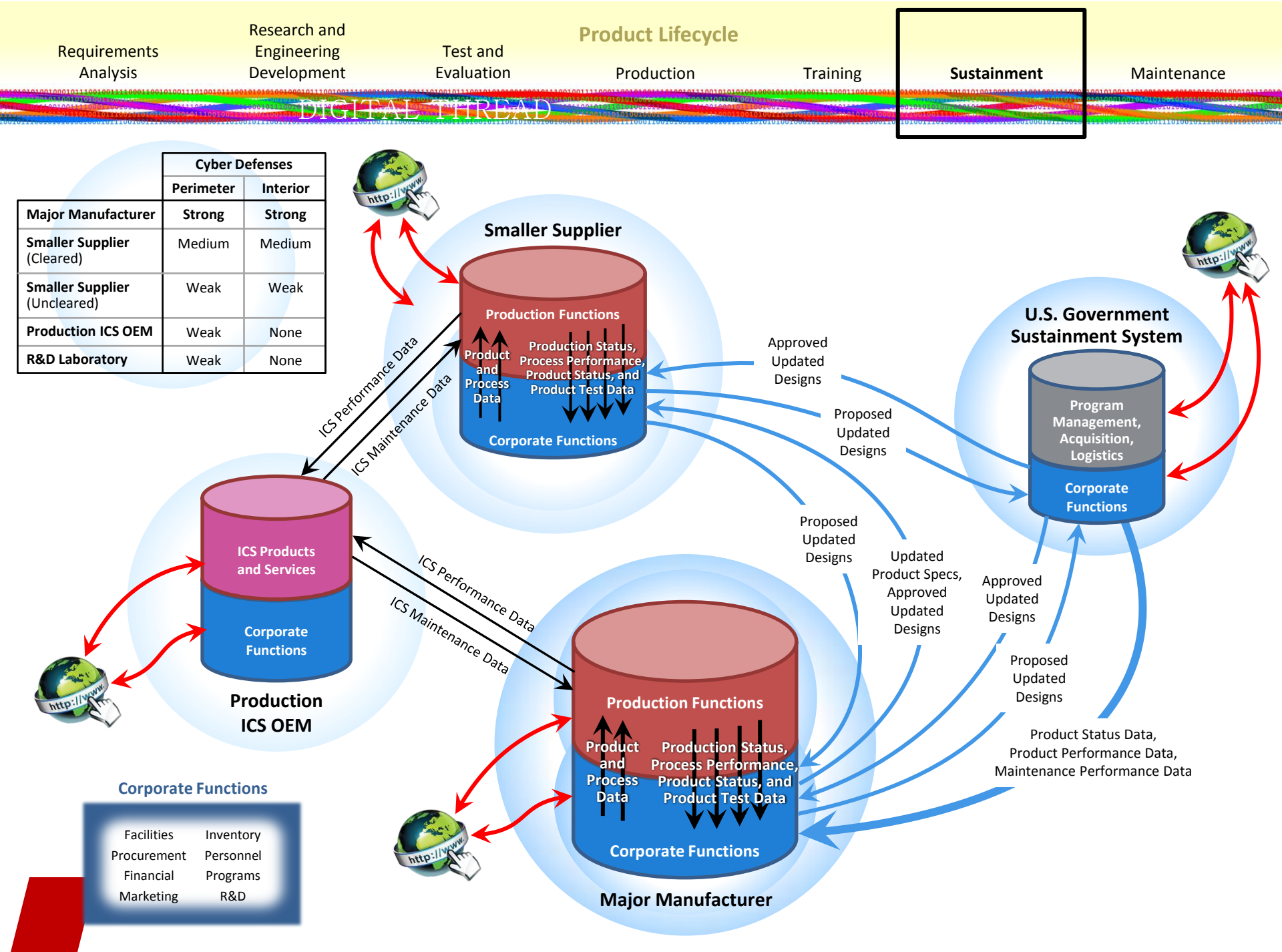
NOTE: This matrix is based on the ISA-95 Functional Model.



Manufacturing Environment Challenges

- Considering both manufacturing and sustainment
- Developing use cases that demonstrate risk / recommendations
- Simplifying ICS guidance for all sizes of organizations
- Addressing human factors incentivizing culture change
- Integrating cyber education into existing delivery network
- Leverage existing technology to mitigate immediate risks / create R&D projects for new technology solutions
- Determine balance of regulation with voluntary measures to achieve greatest benefit


Requirements Analysis
Research and Engineering Development
Test and Evaluation
Production
Training
Sustainment
Maintenance
Product Lifecycle
DIGITAL THREAD
Corporate Functions and Network
Facilities
Procurement
Financial
Marketing
Inventory
Personnel
Programs
R&D
Major Manufacturer
Production Functions and Network
Corporate Functions and Network
1
2
3
4
5
6
Production ICS OEM
ICS Products and Services
Corporate Functions and Network
Maintenance Data
Performance Data
Maintenance Data
Performance Data
Design, Production and Administrative Data
Research Data
Research Data
Research Products
Corporate Functions and Network
R&D Laboratory
Production Functions and Network
Corporate Functions and Network
Smaller Supplier
http://www.
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
1 Product Data
2 Process Data
3 Production Status
4 Process Performance
5 Product Status
6 Product Test Data
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

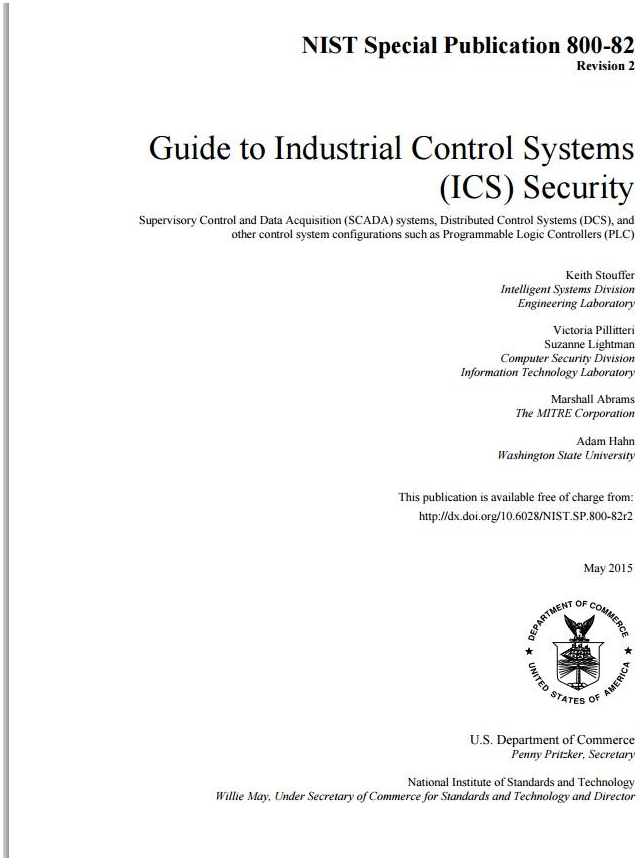

Product Lifecycle
Requirements Analysis
Research and Engineering Development
Test and Evaluation
Production
Training
Sustainment
Maintenance
DIGITAL THREAD
Cyber Defenses
Perimeter
Interior
Major Manufacturer
Strong
Strong
Smaller Supplier (Cleared)
Medium
Medium
Smaller Supplier (Uncleared)
Weak
Weak
Production ICS OEM
Weak
None
R&D Laboratory
Weak
None
Smaller Supplier
Production Functions
Product and Process Data
Production Status, Process Performance, Product Status, and Product Test Data
Corporate Functions
ICS Performance Data
ICS Maintenance Data
Approved Updated Designs
Proposed Updated Designs
U.S. Government Sustainment System
Program Management, Acquisition, Logistics
Corporate Functions
ICS Products and Services
Corporate Functions
Production ICS OEM
ICS Performance Data
ICS Maintenance Data
Proposed Updated Designs
Updated Product Specs, Approved Updated Designs
Approved Updated Designs
Proposed Updated Designs
Product Status Data, Product Performance Data, Maintenance Performance Data
Production Functions
Product and Process Data
Production Status, Process Performance, Product Status, and Product Test Data
Corporate Functions
Major Manufacturer
Corporate Functions
Facilities
Inventory
Procurement
Personnel
Financial
Programs
Marketing
R&D

Use Cases to Demonstrate Risk/Recommendations: Joint Team Development/Review

- **Integrity**
- **Availability**
- **Confidentiality**
- **ICS/Maintenance-specific**

NIST SP 800-82
Keith Stouffer, NIST POC/CFAM MET Member

- **Guide to Industrial Control Systems Security**
  - Provides guidance for establishing secure ICS, while addressing unique performance, reliability, and safety requirements, including implementation guidance for NIST SP 800-53 controls
- **Initial draft - September 2006**
- **Revision 1 - May 2013**
- **Revision 2 - May 2015**



NIST Special Publication 800-82
Revision 2

Guide to Industrial Control Systems (ICS) Security

Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC)

Keith Stouffer
Intelligent Systems Division
Engineering Laboratory

Victoria Pillitteri
Suzanne Lightman
Computer Security Division
Information Technology Laboratory

Marshall Abrams
The MITRE Corporation

Adam Hahn
Washington State University

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-82r2

May 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

Draft CSF Manufacturing Profile URL for Review:

http://go.usa.gov/cuPpG

Cultural/Behavioral Hurdles / Desired Outcomes

- **Hurdles:**
  - People don't want to:
    - Do any more work than needed
    - Take longer than necessary on any task
    - Change
  - Organizations don't want to:
    - Impact production
    - Lessen their competitive stance
    - Lose money
- **Desired behavior**
  - Learn about CFAM
  - Implement technologies and practices to reduce CFAM risks
  - Identify and quickly resolve CFAM incidents
  - Report CFAM incidents so they may be aggregated and shared

Options for Cyber Education Integration: IMEC/DMDII/MEP Award

IMEC, DMDII Awarded $1.2 Million to Fund Advanced Manufacturing Workforce Initiative

September 22, 2016 - Chicago, Illinois - The Illinois Manufacturing Excellence Center (IMEC), Purdue Manufacturing Extension Partnership (Purdue MEP), and the Digital Manufacturing and Design Innovation Institute (DMDII) were named recipients of a $1.2 million award by the U.S. Department of Commerce National Institute of Standards and Technology (NIST) Hollings Manufacturing Extension Partnership (MEP).

The federally funded award supports the efforts of Manufacturing USA, a network comprising nine public-private research institutes, including DMDII, dedicated to advancing manufacturing innovation, education and collaboration. IMEC and Purdue MEP will use these funds to establish "fellows in residence" to work within DMDII to engage small and medium-sized manufacturers on their digital readiness and needs.

"We are in the first wave of a digital revolution in manufacturing. Our pilot framework brings together complementary expertise from the MEP system and DMDII," said Dr. David Boulay, IMEC President. "This collaborative model will address manufacturing priorities through the creation and use of tools and resources that provide manufacturing leaders the roadmap and actions to embrace digital technologies."

"From this award we can continue to proliferate the rise of the digital factory through our unprecedented partnership with the nation's MEP centers," said Haley Stevens, Director of Workforce Development and Manufacturing Engagement at DMDII. "The interconnectedness of manufacturing through data is changing manufacturing jobs. Through technical assistance, this investment provides the necessary resources to assist small and medium-sized manufacturers in preparing for and adopting digital transformations."

Opportunities for Engagement

- **Each working group has broken their questions into research tasks** . . . additional *subject matter experts for interviews and contributors/ reviewers for deliverables still welcomed*
- **Website launched on NDIA portal** . . . *found under Industrial Working Groups*
- **Team reports due in mid-November** . . . *still time to contribute!*
- **Outreach plan developed to share progress** . . . *first public forum was in August, next one planned for November 15th 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*