National Defense Industrial Association

NDIA and DoD Joint Working Group

Cybersecurity for Advanced Manufacturing (CFAM)

NDIA Systems Engineering Meeting
December 9, 2015

Background

NDIA Cyber and Manufacturing Divisions 2014 Joint Working Group

- May 2014 White Paper, "Cybersecurity for Advanced Manufacturing"* had five recommendations for USD(AT&L):
  1. *Work with industry on standards and practices for factory floor cybersecurity*
  2. *Join in industry forums on implementing DFARS 252.204-7012 at factory floor level*
  3. *Update guidance on the Program Protection Plan (PPP) to include protection of critical technical information in factory floor systems*
  4. *Use Red Teams to identify manufacturing system vulnerabilities and gaps in the solution set, and sponsor cybersecurity R&D to fill the gaps*
  5. *Develop programs to facilitate mfg system cybersecurity in defense supply chains.*
- Dec 2014 meeting with Kristen Baldwin (DUSD(SE) office)
  - NDIA will form JWG to work with DoD on these recommendations

Feb 2015 -- Mfg Division suggested SE Division leadership on recommendation 3.

* http://www.ndia.org/Advocacy/LegislativeandFederalIssuesUpdate/Documents/Cyber_for_Manufacturing_White_Paper_5May14.pdf

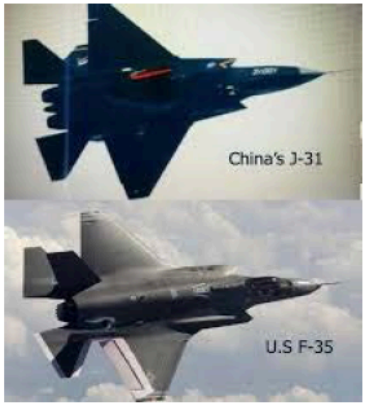
CFAM JWG Objective
(in coordination)

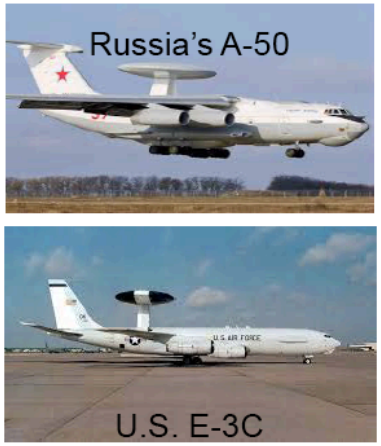
- **Government and industry members of the CFAM JWG collaborate to build on recommendations in the 2014 NDIA white paper, *Cybersecurity for Advanced Manufacturing***
  - Identify cybersecurity vulnerabilities in the manufacturing environment and mitigations . . . *types and boundaries, highest impact 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*

Why This is Important

These are Not Cooperative R&D Efforts

From Brian Hughes' presentation at 2015 NDIA Systems Engineering Conference






U.S. HUMVEE


China's Dongfeng EQ2050


U.S. Reaper


China's Yìlóng-1

Launch Meeting: November 13th

- **34 participants: 9 Government, 8 from membership or academic organizations, 17 company representatives**
- **Engaging discussion between Government and NDIA participants . . .** ***current situation, desired outcomes, barriers, opportunities***
- **Subtopics identified . . .** ***teams formed***
  - Terms of Reference Team
  - Policy Planning and Impacts Team
  - Technology Solutions Team
  - Bounding the Problem for Manufacturing Team
- **Encouraging level of interest and participation**

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?
- **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?
- **Development . . .**
  - What technical solutions can increase cybersecurity in the manufacturing environment?

Next Steps

- **Terms of reference being developed** . . . *Briefing to senior OSD leadership will be scheduled following agreement on TORs*
- **Each working group will elect a team leader and develop their schedule and deliverables** . . . *team leaders will be from industry*
- **Team members may be added throughout the activity as subject matter experts are identified to contribute to the work** . . . *opportunities to get involved*
- **Quarterly full working group meetings** . . . *meeting again in February*
- **Goal is to issue report by December 2016** . . . *will then be coordinated within DoD*

CFAM JWG Members

As of December 7th, 2015

Vicki Barbur
Concurrent Technologies Corp.

Dean Bartles
Digital Manufacturing and Design Innovation Institute

Dawn Beyer
Lockheed Martin Corporation

Brench Boden
AFRL

Megan Brewster
OSTP

Martha Charles-Vickers
Sandia National Laboratories

David Chesebrough
AFEI

Donald Davidson
DoD CIO

Michael Dunn
ANSER

Chris Fall
OSTP

Scott Frost
ANSER

Marilyn Gaska
Lockheed Martin Corporation

James Godwin
BriteWerx, Inc

Jason Gorey
Six O'Clock Ops

Daryl Haegley
OASD (EI&E) IE

Greg Harris
ODASD (MIBP)

David Huggins
Georgia Tech Research Institute

Larry John
ANSER

Thomas McCullough
Lockheed Martin Corporation

Thomas McDermott
Georgia Tech Research Institute

Michael McGrath
McGrath Analytics LLC

Michele Moss
Booz Allen Hamilton

Heather Moyer
Concurrent Technologies Corp.

Catherine Ortiz
Defined Business Solutions

Chris Peters
The Lucrum Group

Robert Pickett
JSJ4, KBLD

James Poplin
Defined Business Solutions

Adele Ratcliff
AT&L MIBP

Melinda Reed
ODASD(SE)

Craig Rieger
Idaho National Laboratory

Frank Serna
Draper

Devu Shila
United Technologies Research Center

Tim Shinbara
The Association for Manufacturing Technology

Joseph Spruill
Lockheed Martin Corporation

Sarah Stern
Boeing, BCA Network Cyber Security

Rebecca Taylor
Nat'l Center for Mfg. Sciences

John Toomer
Boeing

Janet Twomey
Wichita State University

Mary Williams
MTEQ

Jeffrey Wolske
Raytheon

Melinda Woods
AT&L MIBP