NDIA and DoD Joint Working Group

Cybersecurity for Advanced Manufacturing

"Protecting the Digital Thread"

NDIA Manufacturing Division Meeting
October 19th, 2016

Catherine Ortiz, Defined Business Solutions, LLC

Manufacturing is a Cyber-physical Business

Industry Week

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

The Threat is Global and Growing

Manufacturing is an inviting target

NDIA

The Washington Post

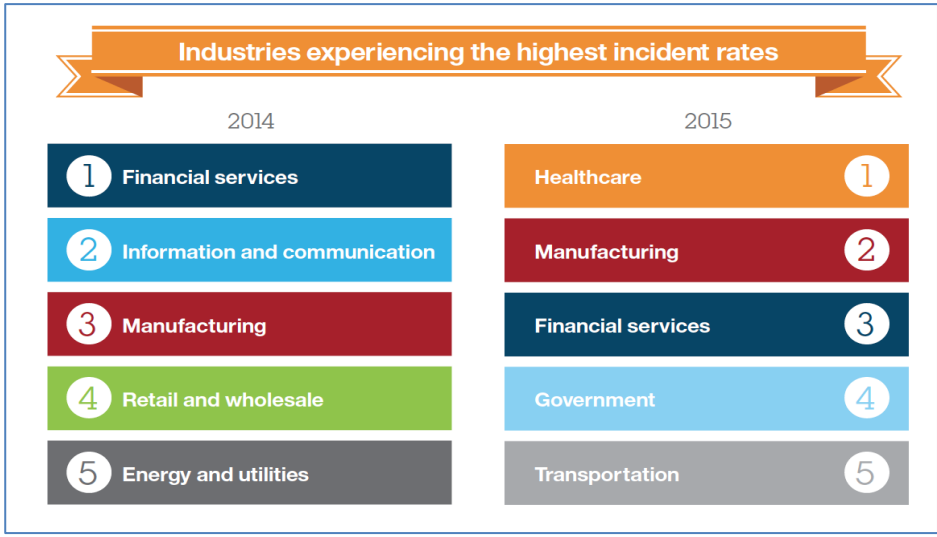
Washington, DC May 28, 2013 Edition: U.S. | Regional Make us your

Weapons designs compromised by Chinese hackers

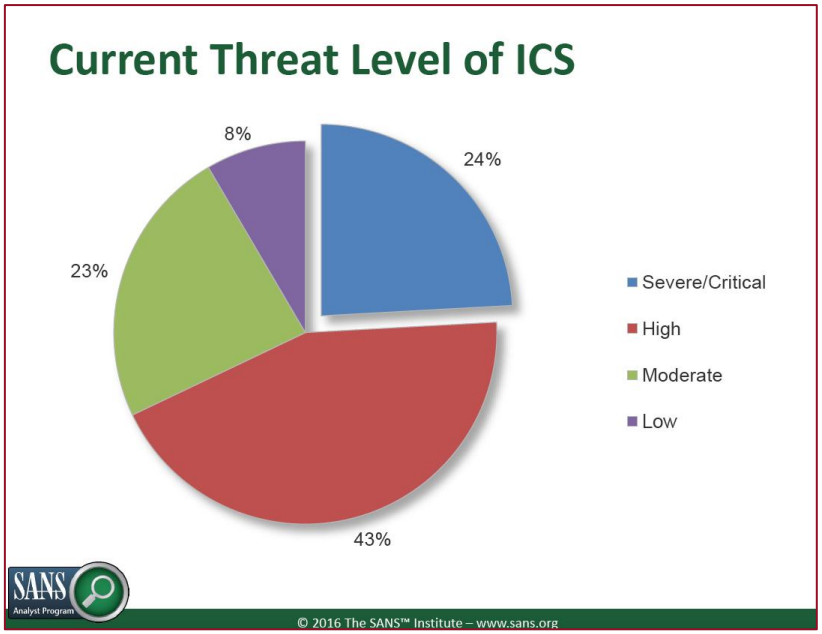
Ellen Nakashima 10:54 PM ET

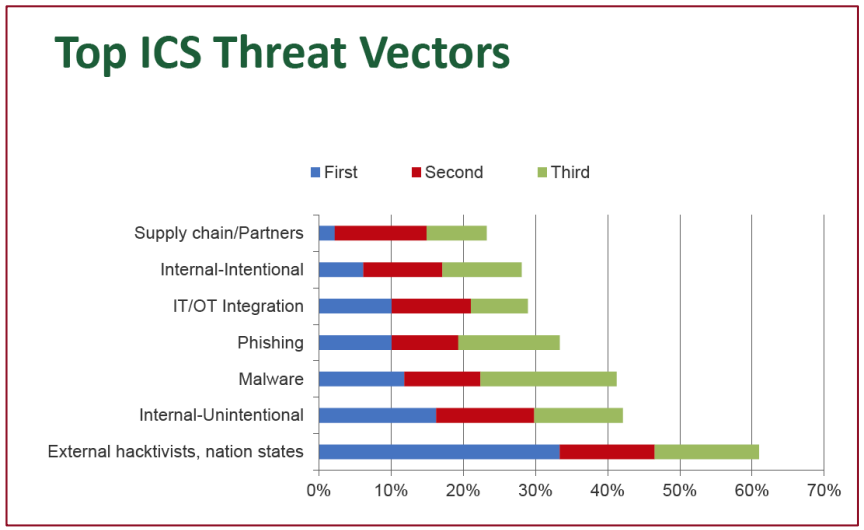
Among more than two dozen U.S. systems breached are programs critical to missile defenses and combat aircraft, according to a confidential report.

- List of compromised designs



IBM Security Services Cyber Security Intelligence Index 2016





SANS 2016 ICS Survey

China's cyber-espionage group: APT1, Unit 61398

Once APT1 has established access, they periodically revisit the victim's network over several months or years and steal broad categories of intellectual property, including technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements, and emails and contact lists from victim organizations' leadership.

-- Mandiant APT1 Report 2013

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

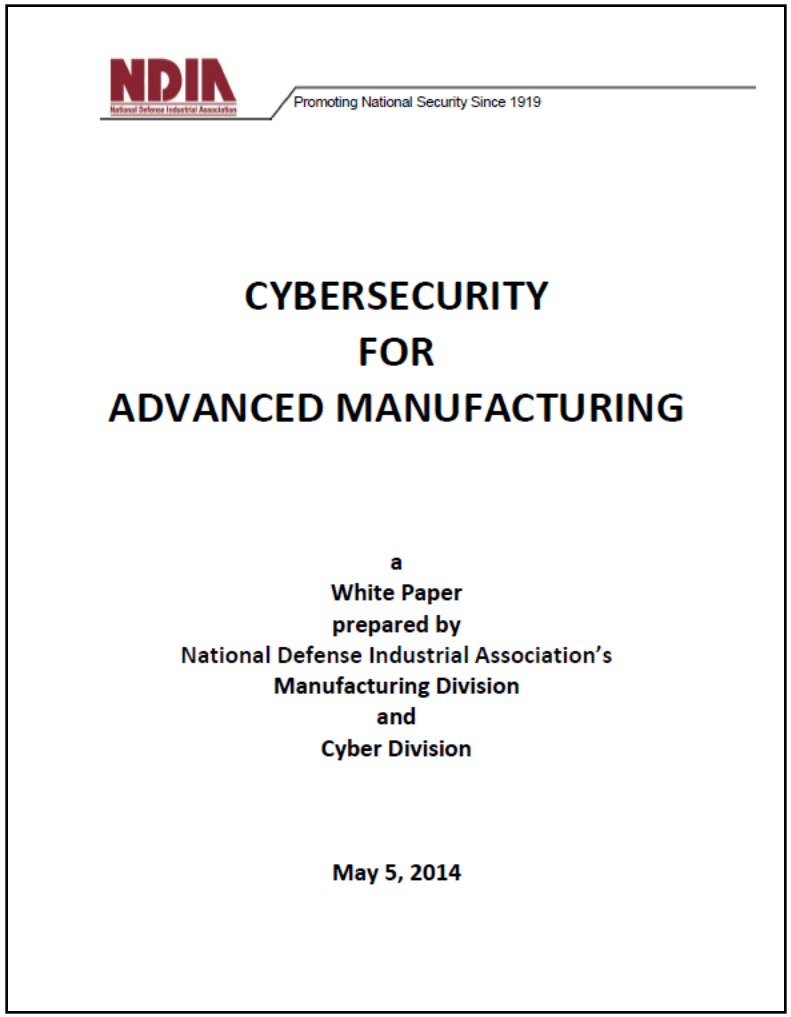

U.S. HUMVEE


China's Dongfeng EQ2050

Distribution Statement A – Approved for public release by DOPSR on 10/21/2015, SR Case # 16-S-0130 applies. Distribution is unlimited.

NDIA White Paper

Protecting the Digital Thread



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?

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
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
  - 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
  - National Institute of Standards and Technology
- **FFDRCs:**
  - Institute for Defense Analyses
  - Sandia National Laboratories
- **Industry member organizations:**
  - National Defense Industrial Association (lead)
  - Association for Manufacturing Technology
  - ASME
  - 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

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 MITRE	**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 ASME	**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	

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 IPDE Systems, LLC	**Anitha Raj** ARAR Technology	**Devu Shila** United Technologies Research Center
Vicki Barbur MITRE	**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

Status & Next Steps

- **Each working group has broken their questions into research tasks** ***. . . subject matter experts are being interviewed and reports are being written***
- **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***