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, Kristen

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.

NDIA is strongly committed to leading the CFAM JWG in collaboration with your office. CFAM JWG members are available to meet with you and OSD leadership as appropriate to provide more information on their activities and receive your guidance on their direction. We appreciate your sponsorship of this important activity.

Sincerely,

Craig R. McKinley
General, USAF (Ret)
President and CEO

Enclosures:
1. Cybersecurity for Advanced Manufacturing White Paper, May 2014
2. Cybersecurity for Advanced Manufacturing Joint Working Group Terms of Reference with Member Roster, February 2016

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

Terms of Reference

**Cybersecurity for Advanced Manufacturing (CFAM)**

*A study by a Joint Working Group of Government representatives and members of the National Defense Industrial Association (NDIA)*

***Objective***

Government and industry members of the Cybersecurity for Advanced Manufacturing (CFAM) joint working group (JWG) will work collaboratively to build on the recommendations in the 2014 NDIA white paper, *Cybersecurity for Advanced Manufacturing.* The CFAM JWG will identify the types and boundaries of cybersecurity threats, vulnerabilities, and consequences in the manufacturing environment and define actions to mitigate those risks. The CFAM JWG will identify ways to incentivize and assist manufacturers (particularly small and medium enterprises (S&ME) in defense supply chains) to improve cybersecurity in manufacturing systems by evolving policies and contract requirements, enhancing security practices, and offering industrial / contractor workforce cybersecurity training. Implementation plans will be developed for the updated courses of action.

***Background***

In 2014, NDIA's Manufacturing Division and Cyber Division jointly developed a White Paper to heighten awareness of the emerging threats, vulnerabilities and consequences in the Industrial Control Systems used in manufacturing, with special attention on defense systems manufacturing. The paper outlines the findings of a 12-month study of the threats to manufacturing specifications and technical data transiting or residing in manufacturing systems, alteration of the data (thereby compromising the physical parts produced), or interference with reliable and safe operation of a production line. The NDIA joint working group recommended actions to better protect the digital thread through which defense systems' unclassified technical information flows during the manufacturing process. Undersecretary of Defense for Acquisition, Technology & Logistics, Frank Kendall, endorsed the recommendations and designated Principal Deputy Assistant Secretary of Defense for Systems Engineering, Kristen Baldwin, to serve as the government sponsor to continue the work.

***Scope***

Review and update actions recommended in the 2014 NDIA white paper, *Cybersecurity for Advanced Manufacturing,* to better protect the digital thread that drives defense systems' manufacturing. Develop implementation plans for the updated courses of action that have been coordinated between government and industry.

***Specific Tasks***

The CFAM JWG will form teams to analyze the multiple facets of manufacturing cyber threats, vulnerabilities, and consequences in the defense industrial base and develop recommendations for actions that will better protect the digital thread. Questions the joint working group will address include:

- What defines a manufacturing environment for the defense industrial base (i.e. within and among the members of defense supply chains)? What are the cybersecurity threats, vulnerabilities, and consequences? How can the cybersecurity risks in manufacturing environments be identified and mitigated?

- What use cases are important across the life cycle of the manufacturing environment? What conditions and practices contribute to cybersecurity or increase cyber risks?

- What actions and activities can improve cybersecurity in the manufacturing environment? What are the activities with the potential to have the greatest near-term impact?

- What types of education, training and awareness of cybersecurity for manufacturing environments are required for existing and future workforces, including workforce leadership? How can cultural and behavior change contribute to increased cybersecurity?

- What existing policies regulations, and standards are applicable to cybersecurity in advanced manufacturing? How do existing policies, regulations and standards need to be augmented, and by whom?

- How can existing network breach reporting and communication processes be improved to increase cybersecurity in manufacturing environments, and by whom?

- What activities implemented inside and outside the Department of Defense, other government agencies or by the private sector can be leveraged to better protect manufacturing networks?

- What technical solutions can be identified, either available now or under development, to increase cybersecurity in the manufacturing environment? What new technology-based concepts should be explored?

***Deliverables***

The CFAM JWG will issue a report by December 2016 for further coordination within DoD and other Government agencies as appropriate.

***Study Organization***

Melinda K. Reed, Deputy Director for Program Protection, Assistant Secretary Of Defense, Research and Engineering (ASD(R&E)) will serve as the government lead in this activity; Catherine J. Ortiz, President, Defined Business Solutions LLC, will serve as the industry lead. The CFAM JWG member list is shown as Attachment A and will be updated as needed. Team members may be added throughout the activity as subject matter experts are identified to contribute to the work.