

NDIA Cybersecurity for Advanced Manufacturing Public Forum

August 18, 2016

Manufacturing Environment Team

Dr. Marilyn Gaska

Manufacturing Environment Team (draft)

- **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

Objective

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

MET focused on the operational environment to address scope and implementation challenges in terms of education and culture change.

Current Status

Deliverable	Status	Comments
Delineation of the manufacturing environments that are to be included in the CFAM effort.		Scope diagram developed using ISA-95 model with all-team concurrence
What defines a manufacturing environment for the defense industrial base?		Diagrams completed including data flows
What are the cybersecurity threats, vulnerabilities, and consequences? How can the cybersecurity risks in manufacturing environments be identified and mitigated?	New Risk WG	Leveraging Keith Stouffer's work at NIST as baseline. Additional SME opportunity
What types of education, training and awareness of cybersecurity for manufacturing environments are required for existing and future workforces, including workforce leadership?	Educa- tion WG	Initial approach developed. Analysis of Alternatives and recommendation to be developed. Additional SME opportunity
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? How can cultural and behavior change contribute to increased cybersecurity?	New Culture / Human Factors WG	Initial approach / plan defined. Additional SME opportunity