

CYBERSECURITY FOR ADVANCED MANUFACTURING JOINT WORKING GROUP FORUM

August 18, 2016

- 7:30am – 8:30am **WELCOME & NETWORKING**
- 8:30am – 8:40am **WELCOME & PREAMBLE**
MG Barry Bates, USA (Ret), *Executive Vice President of Program Development, National Defense Industrial Association*
- 8:40am – 9:20am **KEYNOTE PRESENTATION**
Ms. Kristen Baldwin, *Acting Deputy Assistant Secretary of Defense for Systems Engineering*
- 9:20am – 9:50am **PROTECTING US MILITARY'S TECHNICAL ADVANTAGE: ASSESSING THE IMPACT OF COMPROMISED UNCLASSIFIED CONTROLLED TECHNICAL INFORMATION**
Mr. Brian Hughes, *Director, Joint Acquisition Protection and Exploitation Cell (JAPEC)*
- 9:50am – 10:10am **NETWORKING BREAK**
- 10:10am – 10:55am **DATA BREACH INVESTIGATIONS REPORT**
Mr. John Grim, *Investigative Response Team Lead, Verizon*
- 10:55am – 11:45am **CFAM JWG TEAM LEADERS PANEL**
MODERATOR: Mr. Joe Spruill, *Lockheed Martin*
- ▶ Manufacturing Environment Team, Dr. Marilyn Gaska, *Lockheed Martin*
 - ▶ Technology Solutions Team, Ms. Heather Moyer, *Consultant*
 - ▶ Policy Planning and Impacts Team, Ms. Stephanie Shankles, *Booz Allen Hamilton*
- 11:45am – 12:15pm **OPEN DISCUSSION**
- 12:15pm – 12:30pm **WRAP-UP**
Dr. Mike McGrath, *McGrath Analytics, LLC*

KEYNOTE: MS. KRISTEN BALDWIN, DASD(SE)

Ms. Kristen J. Baldwin is the Principal Deputy to the Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE)). Ms. Baldwin acts on behalf of the DASD and is responsible for engineering and technical workforce, policy, and systems engineering planning for major defense acquisition programs. Her oversight includes concept engineering and analysis, design, development and manufacturing, and independent program review and assessment. She supports the DASD role of functional leader for more than 40,000 defense acquisition professionals in the Department of Defense (DoD) Engineering (ENG) and Production, Quality, and Manufacturing (PQM) workforce. She oversees the DoD strategy for Trusted Systems Design.

A member of the Senior Executive Service (SES), Ms. Baldwin leads modeling and simulation, system security engineering, program protection, system of systems engineering, and systems engineering research and development initiatives. She oversees the DoD Systems Engineering Research Center, a university-affiliated research center dedicated to advancing systems engineering methods, processes, and tools, and the MITRE National Security Engineering Center, a DoD federally funded research and development center.

Ms. Baldwin has been with the Office of the Secretary of Defense (OSD) since 1998, where she has led the application of capabilities-based planning in the acquisition process and served as Deputy Director, Software Engineering and System Assurance. Before working with OSD, Ms. Baldwin served as a science and technology advisor in the Army's Office of the Deputy Chief of Staff for Operations and Plans. Ms. Baldwin began her career at the U.S. Army's Armament Research, Development, and Engineering Center, Picatinny Arsenal.

Ms. Baldwin was a recipient of the Meritorious Presidential Rank award in 2014, in recognition of exemplary service.

Ms. Baldwin received a bachelor's degree in mechanical engineering from Virginia Tech and a master's degree in systems management from the Florida Institute of Technology.

MR. JOHN GRIM, VERIZON

Mr. John Grim, the primary author of the Verizon Data Breach Digest, has over 14 years of experience in conducting digital forensic investigations within the government and civilian security sectors. Currently, Mr. Grim serves on the Verizon RISK Team by leading a team of highly technical digital investigators. In this capacity, Mr. Grim responds to cyber-related security incidents, conducts on-site threat mitigation and breach containment activities, performs digital forensic examinations, and conducts e-discovery and litigation support for customers worldwide.

Prior to joining Verizon, Mr. Grim served 12 years with the U.S. Army investigating security-related incidents; with eight years specifically focused on network intrusion investigations and forensic examinations. Using his knowledge and practical hands-on experience, Mr. Grim has provided computer security related advice, assistance, and formalized instruction to both technical and non-technical audiences. Mr. Grim has also authored or contributed to various policies, procedures, and guides on incident response, evidence handling, forensic examinations, and e-discovery activities.

MR. BRIAN HUGHES, JAPEC

Mr. Brian Hughes is the Director of the Office of the Secretary of Defense (OSD) Damage Assessment Management Office (DAMO) which reports to the Principal Deputy, Deputy Assistant Secretary of Defense for Systems Engineering. The office is responsible for conducting cyber intrusion damage assessments, a coordinated process to determine the effect on defense programs, defense scientific and research projects, or defense warfighting capabilities resulting from compromise of a Defense Industrial Base (DIB) participant's unclassified computer system or network.

Currently, DAMO is developing a joint analysis capability that organizes government (both DoD and interagency) and industry partners to address the risks to the DIB pertaining to the compromise of critical U.S. technologies. The current instantiation

of the joint analysis capability is a Joint Acquisition Protection and Exploitation Cell (JAPEC), which integrates intelligence, law enforcement, counterintelligence, and acquisition community capabilities, policies, and processes. The JAPEC members will develop proactive courses of action to address consequences and to prevent and mitigate future losses.

Before his position with DAMO, Mr. Hughes served as Executive Director of the Defense Science Board for more than 10 years following a career in the U.S. Navy as a submariner serving on fast attack submarines. Mr. Hughes holds a B.S. in physics from Bates College, an M.S. in computer science from George Washington University, and an M.S. in international relations from the London School of Economics and Political Science. He is a member of the Association for Computing Machinery.

DR. MICHAEL MCGRATH, MCGRATH ANALYTICS, LLC

Dr. Michael McGrath is an independent consultant for government and industry technology programs. He is also a Senior Technical Advisor (and former Vice President) at Analytic Services Inc. (ANSER), a not-for-profit government services organization. He recently co-chaired a study of Cybersecurity for Advanced Manufacturing for the National Defense Industrial Association. He previously served as the Deputy Assistant Secretary of the Navy for Research, Development, Test and Evaluation (DASN(RDT&E)), where he was a strong proponent for improvements in technology transition, modeling and simulation, and test and evaluation. In prior positions, he served as Vice President for Government Business at the Sarnoff Corporation, ADUSD for Dual Use and Commercial Programs in the Office of the Secretary of Defense (OSD), Assistant Director for Manufacturing at the Defense Systems Research Projects Agency (DARPA-DSO), and Director of the DoD Computer-aided Acquisition and Logistics Support (CALS) program. While at

DARPA, he managed the Affordable Multi-Missile Manufacturing Program and the Agile Manufacturing program. His early government career included positions in Logistics Management at Naval Air Systems Command and in Acquisition Management in OSD. He is a director of South Carolina Research Authority Applied R&D, a Senior Fellow at the Potomac Institute for Policy Studies, and a member of the National Research Council's Materials and Manufacturing Board, the Defense Materials, Manufacturing and Infrastructure Committee (chair), the Penn State ARL Materials and Manufacturing Advisory Board, and the Georgia Tech Manufacturing Institute Advisory Board.

Dr. McGrath holds a BS in Space Science and Applied Physics and an MS in Aerospace Engineering from Catholic University, and a doctorate in Operations Research from George Washington University.

MR. JOE SPRUILL, CAPT, SC, USN(RET.), CSCP, LOCKHEED MARTIN CORPORATION

Captain Spruill is a familiar face within the National Security arena – career Naval officer, federal civil servant, consultant, and currently a member of the Lockheed Martin team. There he provides support for corporate initiatives and programs in logistics and sustainment.

A graduate of the U.S. Naval Academy, Captain Spruill also completed numerous advanced degrees and executive education programs, and holds professional certifications in logistics and supply chain operations.

Throughout his government and civilian career, he has engaged in supply chain risk management activities; addressing issues like obsolescence, counterfeiting and cybersecurity.

Captain Spruill enjoys working with a number of industry associations, including the National Defense Industrial Association, and the Aerospace Industries Association, in support of Government-Industry collaboration. His favorite work, however, finds him on the water teaching rowing techniques and coaching his crew team.

