Presenter Biographical Sketches

Federal Facilities Council Workshop

The Gates Are Open: Operational Technology and Control System Security for Federal Facilities

Joe Bush is a research mechanical engineer for the U.S. Army Corps of Engineers Engineering Research Development Center, Construction Engineering Research Laboratory (USACE-ERDC-CERL) where he is the Building Energy Systems Team (BEST) team lead for control systems. Since joining CERL in 2002, he has focused on the specification, implementation, and cybersecurity of facility-related control systems (FRCS) with a focus on interoperable multi-vendor open systems.

Mr. Bush has authored multiple Unified Facilities Criteria and Unified Facilities Guide Specifications covering Utility Monitoring and Control Systems, heating, ventilation, and air conditioning controls, and the cybersecurity of FRCS. He supports the USACE Headquarters Engineering and Construction Division as a control system and cybersecurity subject matter expert and serves as the Army member of the Control Systems Discipline Working group for the Tri-Service Standards and Criteria Program.

Mr. Bush is a registered control systems engineer and holds a bachelor's degree in mechanical engineering from The Cooper Union for the Advancement of Science and Art and a master's degree in general engineering from the University of Illinois at Urbana-Champaign.

Nathan Hizer is a registered professional engineer with more than 21 years of federal experience. He currently works in the Veterans Health Administration's (VHA), Healthcare Environments and Facilities Program in the Office of Healthcare Engineering supporting the field in all engineering related issues with a specialty in mechanical engineering and controls. Mr. Hizer has held facilities and engineering roles with the Department of Treasury's Bureau of Engraving and Printing, the Veteran Administration's (VA's) Office of Information and Technology in the Office of Construction and Facilities Management, and with the VA medical centers in Huntington, WV, Prescott, AZ, and Martinsburg, WV. Mr. Hizer has a Bachelor of Science in mechanical engineering from the University of Akron and a Master of Administration with a focus in project management from Northern Arizona University. He holds a Federal Acquisition Certification-Project Management (Senior Level Project Manager) Level III, Contracting Officers Representative Level II certification, Global Information Assurance Certification in Information Security Fundamentals (GISF) and as a Global Industrial Cybersecurity Professional (GICSP). Mr. Hizer is and a licensed professional engineer in the state of Texas.

Jon Huddleston serves as the U.S. Army Corps of Engineers (USACE) Defense Critical Infrastructure (DCI) and Operational Technology Program Manager in the Headquarters USACE Installation Readiness Division (IRD). He conducts and oversees Mission Assurance risk assessments, Simulated Adversary and Threat Replication for Networks (SATRN) cyber threat integration, installation cyber resilience and critical infrastructure dependency studies, exercises, and policy development.
Mr. Huddleston served as Defense Critical Infrastructure Assessment Coordinator for the Army at the Pentagon, NDAA 1650 Cyber Assessment participant and analyst, Mission Analyst and Infrastructure Assessor for Critical Infrastructure Protection-Mission Assurance Assessment Teams supporting Army, Defense Contract Management Agency (DCMA), and the Department of Homeland Security (DHS).
Recognitions include certification as a Certified Business Continuity Professional (CBCP) by the Disaster Recovery Institute International, FBI Infragard member and presenter, recognized by the Director of the Secret Service, and co-authored the program-managed structure for Army control systems and operational technology.

Bob Hunter is a thought leader in the field of securing and managing Operational Technology (OT) including Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems. He previously founded TrendPoint Systems, the leader in data center power monitoring and, NetBrowser Communications, the first DCIM (Data Center Infrastructure Management) system company. He has over 25 years of experience in bringing together successful software and embedded systems projects in the fields of data center infrastructure management, energy management, and cybersecurity management.

Mr. Hunter founded Alpha Guardian using his expertise in the vulnerabilities and securing of key OT and ICS protocols including Modbus, BACnet, SNMP (Simple Network Management Protocol), MQTT (Message Queuing Telemetry Transport), and others. Alpha Guardian is based in San Ramon, California with a research facility located in Spokane, Washington.

Coby Jones is the Senior Manager of Advanced Applications for Johnson Controls Federal Systems. His career with Johnson Controls spans over 25 years. In his current role, he supports information technology and operational technology teams at Department of Defense (DoD) locations and understands the importance of partnership in planning for the Base of the Future. Coby works with federal government customers to guide them through the Digital Transformation process for new and retrofit facility-related control system projects using the latest heating, ventilation, and air conditioning industry technology and cybersecurity practices. He also works as a liaison for DoD customers and Johnson's product development teams to create synergy between new specification requirements and new industry technology. Coby spent 8 years at Fort Liberty Army Installation as a Resource Efficiency Manager, as well as Acting Energy Manager.

Sandy Kline is serving at the Department of Defense (DoD) for the Under Secretary for Acquisition and Sustainment as the Director for Mission Assurance and Facility Related Control Systems Cybersecurity. She is leading efforts to understand, quantify and mitigate the cybersecurity risks to hundreds of thousands of Facility Related Control Systems (FRCS) on military installations worldwide. FRCS represent a significant portion of the Department's critical infrastructure providing the water and power required for accomplishment of military missions. Using the DoD's Mission Assurance methodology as foundation, Ms Kline is working across the Department to enable the identification of the impacts of cybersecurity attacks to the operational technology (OT) and information technology (IT) to mission capabilities and to the life, health, and safety of installation personnel. Key to this effort is mapping interdependencies between and across systems by building on mission decomposition work the Services have done through Crown Jewel, NDAA 1650, and Mission Relevant Terrain-Cybersecurity analyses. Leveraging the NIST Cybersecurity Framework 2.0 (release in February 2024), her team has created a FRCS Cybersecurity Framework to enable standardized assessment and tracking of organizational cybersecurity maturity that is key the development and sustainment of complex continuous monitoring and recovery capabilities being pursued by DoD to meet Executive Order 14028 Improving the Nation's Cybersecurity.

Recent achievements by her office include the release of updated construction criteria for FRCS; completion of Cybersecurity Resilience Readiness Exercises at Marine Corps, Navy, and Army installations; establishment of the FRCS Cyber Framework; partnerships with Industry to update military construction guidance for cybersecurity commissioning; and engagement with the National Security Agency to incorporate intelligence informed cybersecurity requirements into legacy and new FRCS systems.

Prior to working for DoD, Ms. Kline worked for the Secretary of the of Navy as the Director for Installation Resilience working on mission assurance energy, water, and cybersecurity resilience issues that resulted $250M in energy savings and $300M in clean air credits used to improve energy and water resilience and achieve objectives of Executive Order 14027. Ms. Kline has also been the Deputy Director for Military Construction and Deputy Chief Information Officer and Enterprise Architect for the Naval Facilities Engineering Command, the Director for Enterprise IT at the Naval Sea Systems Command, and the Program Manager for Logistics for the F-14 aircraft at the Naval Supply Systems Command as has been recognized in all these position with Navy Meritorious Civilian Awards.

Ms. Kline is a graduate of the Pennsylvania State University as an Industrial Engineer and lives in Alexandria with her husband and dogs and has one daughter.

Michael Powell is a cybersecurity engineer at the National Cyber-Security Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) in Rockville, Maryland. His research focuses on cybersecurity for the manufacturing sector, particularly how it impacts industrial control systems.

Dr. Powell joined the NCCoE in 2017. In his previous positions, he was responsible for the management and oversight of the building and commissioning of the U.S. Navy's Arleigh Burke-51 class ships. He also served in the Navy for over 20 years, retiring as a Chief Petty Officer. He holds a bachelor's degree in information technology, a master's degree in public administration, and a master's degree in information technology. Dr. Powell completed his doctorate in applied computing at Pace University in Westchester, New York.

Tom Smith is currently serving at the General Services Administration (GSA) as the Services Center Director in the information technology (IT) Category, Office of Supply Chain Risk Management (SCRM) where he has been leading recent efforts to build collaborative working relationships across Federal Acquisition Service (FAS), industry, and government agencies to improve compliance and integration of Cybersecurity Supply Chain Risk Management (C-SCRM) policies, processes, and capabilities to strengthen and secure GSA-wide contract vehicles. He joined the GSA team in 2018 as a member of the IT category management team serving as a senior IT Specialist and SCRM subject matter expert within the Office of IT Solutions. His accomplishments include developing and establishing various C-SCRM training programs for the acquisition workforce, piloting multiple SCRM tools in use across FAS, and creating vehicles for our strategic customers to include, the benchmark Second Generation IT program, the Ascend cloud marketplace, and current Supply Chain Risk Illumination Professional Tools & Services (SCRIPTS) blanket purchase agreement efforts. Tom continues to be engaged in every aspect of building and maturing the FAS C-SCRM program, SCRM Division, and providing valued C-SCRM subject matter expertise both within GSA and across the federal government.

Prior to joining GSA, Tom served in a variety of senior acquisition corps leadership roles during his nearly 30 years of Air Force active duty and federal civil service. His roles ranged from Chief Engineer for the Air Force's Business Enterprise Services Division—with technical oversight of $30 billion in Air Force enterprise-wide strategic sourcing and services—to Deputy Director and military command positions in numerous major defense acquisition programs delivering war-winning capabilities in weapons, aircraft, avionics, and space launch systems. His military awards include both the Defense Meritorious Service Medal, Meritorious Service Medal, and Joint Service Commendation Medal.

Tom holds senior acquisition certifications in program management, systems engineering, and information technology. He holds a bachelor's degree in electrical engineering from Auburn University and a Master of Science degree in engineering management from the Florida Institute of Technology. He and his wife, Liz, live in Auburn, AL, and have three grown children, Mary, Thomas, and Lauren.

Chuck Weissenborn works at Dragos, an industrial cybersecurity company—working with operational technology, industrial control systems, and the industrial internet of things—on a mission to safeguard civilization. As the Chief Technology Officer for Dragos Public Sector, he leads the company's efforts to support public sector organizations around the world and their efforts to secure control systems and associated operational technologies. Before joining Dragos, Mr. Weissenborn worked at Symantec where he was responsible for all business operations supporting the U.S. Army worldwide.

Mr. Weissenborn is also a member of the Army National Guard as a member of the Critical Infrastructure Protection Battalion (CIPBN) in the West Virginia National Guard. The CIPBN provides mission assurance assessments and risk reduction recommendations across the Department of Defense (DoD) including teams aligned to the Headquarters of the Department of the Army G3-5-7, the Defense Information Systems Agency. In his Guard role, he often supports Joint, Army, and inter-agency efforts to bring together community partners and private sector utilities to ensure the successful execution of public sector mission sets that rely on operational technology.

Before joining the West Virginia National Guard, Mr. Weissenborn was a member of the Texas National Guard for over 18 years, with assignments that included the S6 Non-commissioned Officer in Charge for the 36th Combat Aviation Brigade and the Texas Defensive Cyber Operations Element. He most recently returned from a deployment to the U.S. Central Command area of responsibility where he supported the long-range precision fires mission. Mr. Weissenborn has deployed four times in support of military operations since September 11, 2001.

Mr. Weissenborn is an avid supporter of several non-profit organizations and is the co-chair of the Critical Infrastructure/Control Systems cybersecurity committee at the National Defense Industrial Association (NDIA). NDIA supports engagement and collaboration efforts between the DoD and the defense and organic industrial base.

Mr. Weissenborn lives in Annapolis, Maryland with his wife Caitlin, and children: Eleanor, Bruce, Wally, and Calleigh.