DOD ACHIEVING RESILIENCE FOR CONTROL SYSTEMS ACROSS GOVERNMENT-OWNED AND COMMERCIALLY-OWNED ASSETS

TUESDAY: SESSION 2, TRACK 2

SESSION CHAIR / MODERATOR

Aleksandra Scalco, US Navy

PANELISTS

- Michael Dransfield (SES), NSA, *National Security Memo*
- Daryl Haegley, OSD Policy, *Executive Office (EO) 100-day Sprints*
- Sandra Kline (SES), ASN EIE, *Systems Owner EIE*
- Michael Kilcoyne, NAVFAC DCIO/CTWH, *System Owner NAVFAC*
- Steve Simske, Professor of Systems Engineering, Colorado State University, *Security Approaches*

SESSION ABSTRACT

Resilience capability for control systems traverses government-owned and commercially-owned assets. Both government-led and industry-led initiatives seek to address aspects of achieving resilience capability such as National Defense Authorization Acts (NDAA) addressing various policy aspects related to cyber defense of control systems. Consistency among stakeholders on how to describe control system challenges and attributes will help industry better understand challenges. For the government, authorities are distributed among agencies such as the Department of Energy (DOE) for power infrastructure, Department of Homeland Security (DHS) for state, local and tribal environments, and within the Department of Defense (DOD), and U.S. Cyber Command (USCYBERCOM) for cyber effects, as well as other agency entities. Similarly, in the commercially-owned asset sector, there are varying oversight and governance authorities. The purpose of this panel is to discuss some of the emerging concepts to achieve greater resilience for control systems from Zero Trust architectures to shared situational awareness, modeling and simulation capabilities, and the need for consistency of terms used to describe these challenges.