Cybersecuring Facilities and Facilities Systems - National Academy of Sciences (NAS)
Federal Facility Council (FFC) – May 2015

The National Research Council (NRC) part of the National Academy of Sciences (NAS) Federal Facilities Council (FFC) will host a three-day workshop in May 2015 to promote awareness and share solutions to cyber secure government and commercial facilities and supporting infrastructure.

Potential nation-state cyber-attacks on the US electrical power grid continue to threaten to disrupt facilities and their supported mission / business. More complex and frequent Advanced Persistent Threat (APT) cyber-attacks on facility-related control systems continue to evolve into a mature danger. Significant cyber vulnerabilities exist in the US electrical power grid, in embedded computers (such as those in facilities' air conditioners, elevators, and security alarms), and in associated building automation and energy management systems.

The Federal Facility Council will host three full-day workshops between private and public-sector cybersecurity, electric power grid and federal facility managers to share best practices for improving resilience of government / commercial facilities in the event of cyber-attack on the commercial power grid and energy management control systems. Goal of the workshops: Consolidate guidance, solutions, experts and practitioners, share best practices, and characterize facility cybersecurity resource requirements and gaps in legislation.

**Invited keynote speakers:
Honorable Senator John McCain
Michael Daniel, Special Assistant to the President and Cybersecurity Coordinator
Admiral Mike Rogers, Commander, U.S. Cyber Command (USCYBERCOM)
Dr. Phyllis Schneck, Deputy Under Secretary for Cybersecurity for the National Protection and Programs Directorate (NPPD), Department of Homeland Security

Where: National Academy of Sciences Building, 2101 Constitution Avenue, NW | 202-334-2000

Who: Inclusive of the Federal fFacility community, with no attendance fee. Invited attendees will include cybersecurity practitioners, technical leaders, and risk owners from Facilities community, as well as key stakeholders and thought leaders from the broader scientific and information security communities.

Program: Each day will include keynotes, expert speakers, panels and significant interaction. Focus for 2015 is on the cybersecurity challenges facing Federal Facilities professionals, the many complex issues involved, training and networking opportunities. Sessions designed for both technical and management audiences, Facility Engineers / Managers, Network Specialists, etc. Agenda will be updated frequently.

Workshop day #1: Provide overarching landscape - from GRID / utility service provided to facility smart meter / devices; Outline applicable Govt / policies & industry best practices; How to map industrial controls systems (ICS) and building automation systems (BAS) to critical processes & apply risk management aligned to mission assurance processes; Overview of tools to discover, assess, continuously monitor networked or stand-alone embedded digital device systems

Workshop day #2: Commercial / Industry / Vendors demonstrate solutions facility managers can implement to safeguard federal facilities and ICS/BAS from a cyber-attack, including options for legacy, current and future technologies; Review of laboratory & centers of excellence capabilities.

Workshop day #3: Recommendations for cybersecurity language to bolster acquisition, contracts, budgeting, sustainment planning, business case analysis, etc.; provide templates

Concurrently, DHS ICS CERT will provide adjoining 1/2 day and full day CSET hands-on demo / training session on site or at another location.