Day 1, Nov 17, 2015

8:00 a.m. – 9:00 a.m. **Check in/Setup**

9:00 a.m. – 9:10 a.m. **Welcome and Introductions**

9:10 a.m. – 9:30 a.m. **Federal Perspective Keynote – *Global/National Landscape*:** Former Congressman Steve Stockman

- Overarching commentary on cyber legislation and challenges (privacy, encryption, information sharing)

Topic 1 – Policy and Governance:

9:30 a.m. – 9:50 a.m. DHS - NPPD/Office of Cyber and Infrastructure Analysis - Susan Stevens

- National Protection and Programs Directorate (NPPD) efforts to address the needs of all 16 Sectors to understand and manage cybersecurity risks for the multitude of facility and building types

9:50 a.m. – 10:10 a.m. DoD CIO - Kevin Dulany

- DoD adoption and implementation of Risk Management Framework, creating a Master List of facility-related control systems

10:10 a.m. – 10:30 a.m. **Break**

Topic 2 – Building Control System Vulnerabilities:

10:30 a.m. – 10:50 a.m. DHS - NPPD/Office of Cybersecurity and Communications/ICS-CERT - Marty Edwards

- Building Control System cyber threats and vulnerabilities; role of ICS-CERT

10:50 a.m. – 11:10 a.m. Interagency Security Committee, Federal Aviation Administration – Will Morrison

- Overview of the ISC White Paper, "Securing Government Assets through Combined Traditional Security & IT"

Topic 3 – Cyber Efforts for Federal Facilities:

11:10 a.m. – 11:30 a.m. DOE - Joe Hagerman

- Building Cybersecurity Framework for utilities, building owners/operators, and vendor supply chain; optimizing cybersecurity to enable increasing use of 'smart' equipment to provide significant energy savings and other consumer benefits.

11:30 a.m. – 11:50 a.m. NIST – Keith Stouffer

- Release of NIST SP 800-82 R2 major highlights, Section 2.5 for Building control Systems, Control Systems Lab Overview

11:50 a.m. – 12:00 p.m. USCYBERCOM – Bob Leverton

- Overview of Joint Base Architecture for Secure ICS (J-BASICS) Tactics, Techniques & Procedures (TTPs)

12:00 p.m. – 12:15 p.m. **Q&A for Morning Topic Speakers**

12:15 p.m. – 1:30 p.m. **Lunch**

1:30 p.m. – 1:50 p.m. **DoD Keynote – *DoD Installation Landscape*** John Conger ASD Energy, Installations & Environment

- Senior Executive perspective

Topic 4 – Federal Cybersecurity Acquisition/Budgeting/Design Requirements:

1:50 p.m. – 2:10 p.m. GSA - Emile Monette

- GSA-DoD Acquisition Reform Report, follow on FAR and DFAR procurement language, future initiatives – GSA perspective

2:10 p.m. – 2:30 p.m. DoD CIO - Don Davidson

- GSA-DoD Acquistion Reform Report, follow on FAR and DFAR procurement language, future initiatives – DoD perspective

2:30 p.m. – 2:50 p.m. GSA – Jeff Koses

- Considerations in acquisition rule-making for cyber status of IT acquisition cadre play of different GSA schedules in access systems

2:50 p.m. – 3:00 p.m. Whole Building Design Initiative: Rick Tyler, US Navy

- Overview of draft Unified Facility Criteria 4-010-06 CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS

3:00 p.m. – 3:15 p.m. **Break**

Topic 5 – Government Tools for Discovery & Assessment:

3:15 p.m. – 3:35 p.m. NSA GrassMarlin - Jerome Crocker

- Overview of the GrassMarlin passive network discovery tool, future enhancements

3:35 p.m. – 3:55 p.m. DHS ICS-CERT CSET - Barry Hansen

- Overview of the DHS-ICS CERT Cyber Security Evaluation Tool (CSET), future release enhancements

3:55 p.m. – 4:15 p.m. Cyber Ranges - DoD National Cyber Range – Dr. Robert Tamburello

- Overview of Control System Test and Evaluation Events at the DoD National Cyber Range

4:15 p.m. – 4:30 p.m. **Q&A for Afternoon Topic Speakers Action Item Review / Adjourn**

Day 2, Nov 18, 2015

8:00 a.m. – 9:00 a.m. **Check in/Setup**

9:00 a.m. – 9:20 a.m. **Vendor Perspective Keynote 1 – *Commercial Landscape*:** Alan Wade - Wade Associates

- A career intelligence perspective on current and future cyber threats

Topic 6 – Continuous Monitoring Solutions:

9:20 a.m. – 9:50 p.m. Preston Futrell – NexDefense

- Overview of Sophia passive monitoring continuous monitoring tool developed by INL, now commercialized

9:50 a.m. – 10:10 a.m. Billy Rios – WhiteScope

- Overview of Building Automation Systems continuous monitoring solutions, enumeration of internet-facing BAS using Shodan

10:10 a.m. – 10:25 a.m. **Break**

Topic 7 – Tools for Discovery, Assessment:

10:25 a.m. – 10:45 a.m. Jason McHuen – Parsons

- Hands-on demonstration of Kali Linux, Metasploit targeting and attacking Building Control Systems

10:45 a.m. – 11:05 a.m. Jonathon Butts - QED Secure Solutions

- Security of BAS installed by third-party integrators – identification, acquisition and security strategy implementation

Topic 8 – Training, Equipping and Certifying the Facility Cyber Workforce:

11:05 a.m. – 11:25 a.m. NIST NICE - William Newhouse

- Overview of the NIST National Initiative for Cyber Education (NICE)

11:25 a.m. – 11:55 a.m. Michael Assante - SANS Institute

- Overview of the current cybersecurity certification landscape; incorporating control system uniqueness

11:55 a.m. – 12:00 p.m. **Q&A for Morning Topic Speakers**

12:00 p.m. – 1:00 p.m. **Lunch**

1:00 p.m. – 1:20 p.m. **Vendor Perspective Keynote 2 – *View from the Field*:** Ron Zimmer – CABA

- CABA's Intelligent Building research project

Topic 9 – View from the Field:

1:15 p.m. – 1:35 p.m. Alex Tarter – Ultra Electronics, 3eti

- Cybersecuring Control System End-Point devices

1:35 p.m. – 1:55 p.m. Robert Young – Parsons

- Managing Physical Access Control Systems and Electronic Security Systems

1:55 p.m. – 2:15 p.m. Jorge Lozano – Condortech Services

- Integrating multiple Building Control System challenges

Topic 10 – Threat Info Sharing:

2:15 p.m. – 2:45 p.m. Jon Miller – Cylance

- Operation Cleaver, how the Iranian campaign unfolded, and the ease with which they exploited Control Systems

2:45 p.m. – 3:00 p.m. **Break**

Topic 11 – Vendor Capability "Fast Pitches" (3 minutes per vendor)

3:00 p.m. – 4:15 p.m.

Condortech Services	Chinook Systems	MissionSecure	Migrate2	QED Secure Solutions
Parsons	Honeywell	Power Engineers	Langer Group	Peregrine Technical Solutions
Siemens	Schweitzer Engineering Laboratories	Johnson Controls	FireEye	TCecure
OSIsoft	Schneider Electric	Ultra Electronics, 3eTI	Bentley	Tempered Networks
		Distributed Information Technologies		

4:15 p.m. – 4:30 p.m. **Action Item Review / Adjourn**

Day 3, Nov. 19, 2015

Optional Training / Demonstrations:

National Academy of Science Building - 2101 Constitution Ave., Wash DC - Member's Room

<<BRING YOUR OWN LAPTOP>>

Registration link:

https://www.eventbrite.com/e/optional-training-demonstrations-cset-grassmarlin-ffc-workshop-cyber-resilience-of-building-control-tickets-19302931588

9:00 a.m. – 11:00 a.m. DHS/ICS-CERT Cyber Security Evaluation Tool (CSET)

CSET is a desktop software tool that guides users through a step-by-step process to assess their control system and information technology network security practices against recognized industry standards. The output from CSET is a prioritized list of recommendations for improving the cybersecurity posture of the organization's enterprise and industrial control cyber systems. CSET has been designed for easy installation and use on a stand-alone laptop or workstation. It incorporates a variety of available standards from organizations such as National Institute of Standards and Technology (NIST), North American Electric Reliability Corporation (NERC), International Organization for Standardization (ISO), U.S. Department of Defense (DoD), and others. CSET provides an excellent means to perform a self-assessment of the security posture of your control system environment. <<CDs to be provided at FFC Workshop>>

12:00 p.m. – 2:00 p.m. NSA GrassMarlin Network Discovery Tool

In support of a passive means to generate a Control System network and discover IP devices, NSA has developed the GRASSMARLIN (GM) tool. GRASSMARLIN is a software prototype that provides a method for discovering and cataloging SCADA (Supervisory Control and Data Acquisition) and CS (Control System) systems on IP-based networks. GRASSMARLIN uses a variety of sources to generate this data, including PCAP files, router and switch configuration files, CAM tables and live network packet captures. The tool can automatically determine the available networks and generate the network topology as well as visualize the communication between hosts. GRASSMARLIN is still in a prototype phase.

GrassMarlin has been approved for Open Source distribution. <<CDs to be provided at FFC Workshop>> The GM POC is Jerome Crocker.

A GM Plug-In has been integrated into the DHS ICS-CERT Cyber Security Evaluation Tool (CSET) 6.2 released January 2015. When installing the tool, use Custom Install and select the GM Plug-In option. If you need assistance and/or technical support with CSET and GM Plug-In, contact Barry Hansen or Michael Chipley.