SCADA/IOT Panel

This panel will focus on innovative & emerging solutions and remaining challenges in the cybersecurity of industrial control systems ICS/SCADA. Representatives from government and infrastructure providers will talk about major efforts that are providing greater levels of protection for our Critical Information Infrastructure. New levels of collaboration, technology that reaches well beyond current solutions, and the generation of new resiliency tactics will be offered. Remaining challenges for work in both government and industry will also be addressed.

Panelists

Moderator: Dr. John H. Saunders, MITRE Corporation

Panelist	Topic	Vita
Daryl Haegley OCO, CCO; **OASD Energy, Installation & Environment**	Facility Related Control Systems	Mr. Haegley overseas DoD policy development, cybersecurity assessment requirements and system authorization process improvement for Control Systems / Platform Information Technology systems. Additionally leads the generation of the Control Systems cybersecurity scorecard, Cybersecurity of Facility Control Systems Unified Facilities Guide, cyber range requirements and the DoD processes and integrate capabilities needed to systematically track, analyze, secure and report facility energy and related data. He maintains four certifications, three Masters' degrees, two college tuitions & one patent.
Craig Lightner **Washington Gas & Light**	Securing Natural Gas Distribution	Mr. Lightner was a system integrator for Industrial Control Systems (ICS) for 26 years providing SCADA systems for utilities, industrial and chemical processes. He occupies the role of Supervisor of Automation and Control for the Washington Gas and Light utility headquartered in Washington DC and has done so for 14 years. During his tenure with WGL the ICS has evolved into a cyber protected infrastructure employing many of the latest technologies and methodologies. The WGL infrastructure has been reviewed and endorsed by DHS for best cyber practices.

DHS ICS-CERT Organization

National Cybersecurity and Communications Integration Center (NCCIC)

Mission

Assisting critical infrastructure asset owners to reduce the risk of impacts from cyber attacks and events by assisting them to improve their cybersecurity defensive posture and respond to incidents and emerging threats/vulnerabilities.

Risk Reduction

- ICSJWG
- Training
- Assessments
- Tools - CSET

Operations

- Incident Response
- Vulnerability Coordination
- Situational Awareness
- Technical Analysis

Benefits

- Awareness of emerging threats
- State of the art analysis
- Incident response support
- Established partnerships
- Collaboration with other agencies and partners

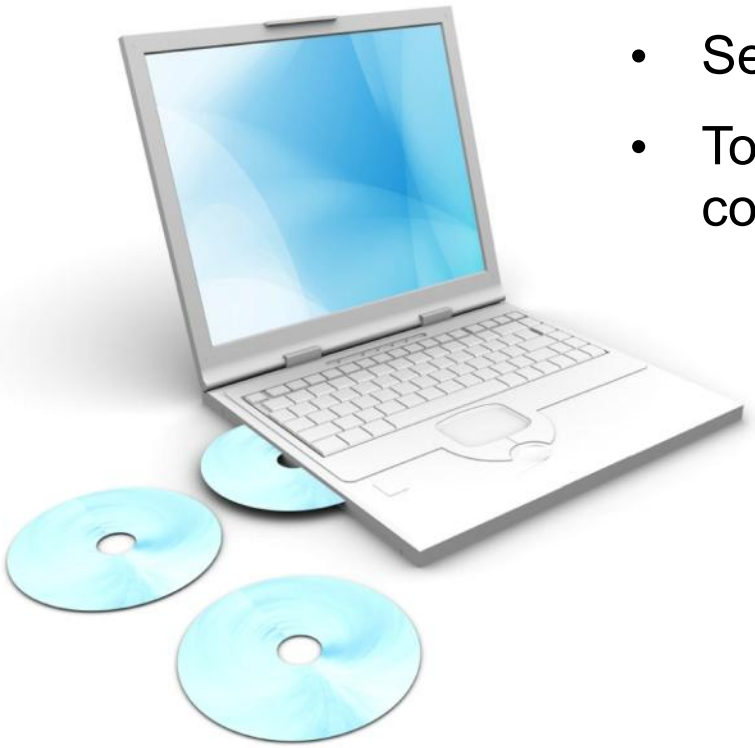
Partners: ISACs, Asset Owners, IC, LE, Agencies, Associations, International

Products: Situational Awareness

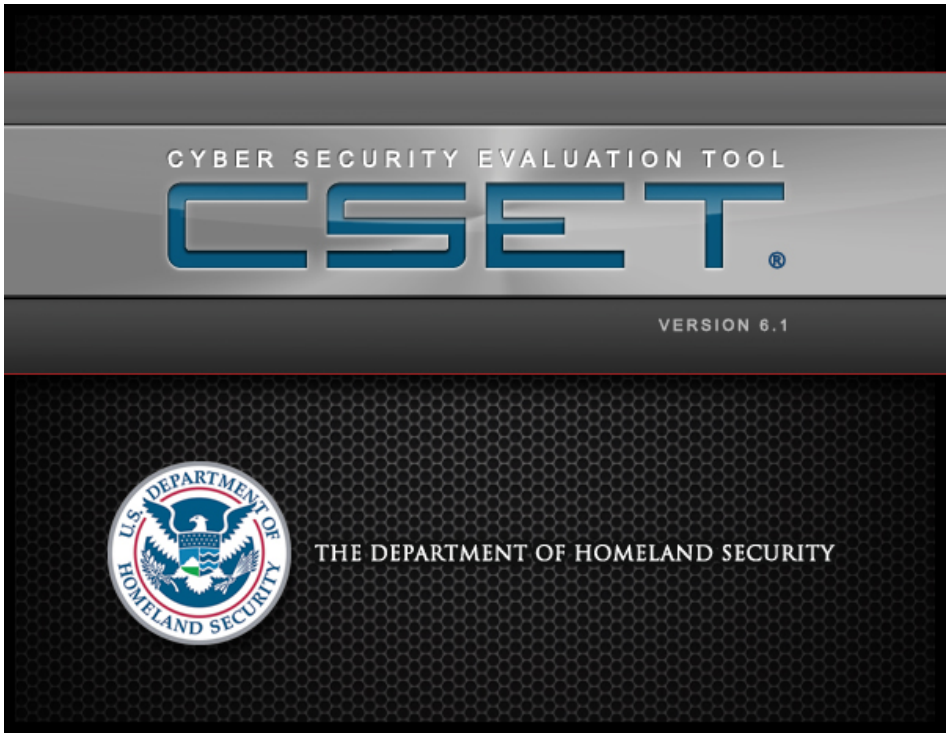
- Threat actor indicators in the form of Alerts, Advisories, and Indicator Bulletins
- Advanced analysis capabilities to provide actionable information about:
  - Malware
  - Spear-phishing emails
  - Compromised hosts
  - Lateral movement of threat actors

- ICS-CERT's Perspective:
  - Broad vision of threat landscape
  - Ability to correlate specific incidents with previous threat actor activity
  - Actionable Intel and coordination with IC and Law Enforcement

Cyber Security Evaluation Tool



- Stand-alone software application
- Self-assessment using recognized standards
- Tool for integrating cybersecurity into existing corporate risk management strategy



CSET Download:

us-cert.gov/control_systems/csetdownload.html

Assessments: On-Site Support

- **Cyber Security Evaluation Tool (CSET):**
  - Assists critical infrastructure asset owners in conducting self-assessments.
- **Design Architecture Review (DAR):**
  - Provides a comprehensive evaluation and discovery process, focusing on defense strategies associated with an asset owner's specific control systems network.
  - Includes an in-depth review and evaluation of the control system's network design, configuration, interdependencies, and its applications.
- **Network Architecture Validation and Verification (NAVV):**
  - Provides a sophisticated analysis of the asset owner's network packet-data.
  - Passively analyzes data and develops a detailed representation of the communications flows and relationships between devices.

ICS-CERT Incident Response

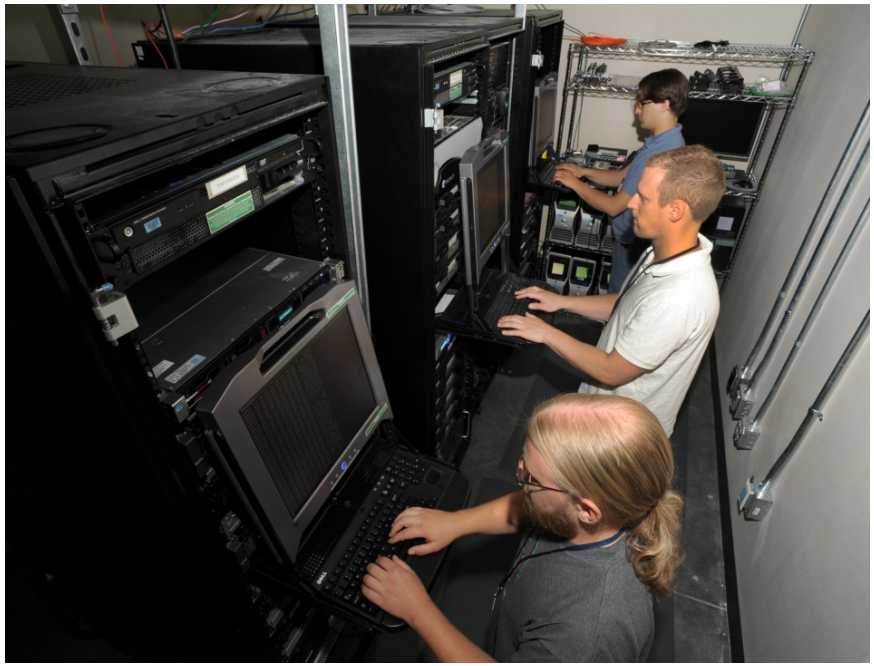
- **Assist asset owners**
  - Onsite incident response teams
  - Host based intrusion detection
  - USG provided indicators
  - Network architecture
  - Data collection
  - Mitigation
- **Offsite technical analysis teams**
  - Analysis of collected data
  - Customer reporting
- **Providing a unique perspective of the threat landscape and associated defensive strategies**

Advanced Analytic Lab

Provides cyber expertise and services in support of ICS-CERT

Capabilities include:

- Malware analysis
- Forensic analysis
- Incident response
- Vulnerability verification
- Patch validation
- Control systems test bed environment
- Embedded device forensics



Available Training

Web-based Training

- Operational Security for Control Systems
- Cybersecurity for Industrial Control systems

Instructor-led Courses

- Introduction to Industrial Control Systems Cybersecurity
- Intermediate Industrial Control Systems Cybersecurity (lecture only)
- Intermediate Industrial Control Systems Cybersecurity (hands-on)
- Industrial Control System Red/Blue Cybersecurity Training

(Access ICS-CERT Web Based Training at http://www.ics-cert.us-cert.gov <Training>)

ICS-CERT Contact Information

Industrial Control Systems Cyber
Emergency Response Team (ICS-CERT)

ICS-CERT@hq.dhs.gov

Phone: (877) 776-7585

Web: https://ics-cert.us-cert.gov/