Jeff Gray – Unit Chief, Training and Outreach

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
National Cybersecurity and Communications Integration Center (NCCIC)
ICS-CERT Organization

Mission

Risk Reduction
- ICSJWG
- Training
- Assessments
- Tools - CSET

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.

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

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

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

UNCLASSIFIED//FOR OFFICIAL USE ONLY
Assessments: On-Site Support

- ICS-CERT uses the CSET to assist critical infrastructure asset owners in conducting self-assessments
  - 50 assessments in multiple sectors in FY-2010
  - 80 assessments in FY-2011
  - 85 assessments in FY-2012
  - 72 assessments in FY-2013 (#’s affected by sequestration)
  - 46 assessments in FY-2014 (as of May 7, 2014)

- Assessment teams assist infrastructure asset owners in all sectors to identify gaps in their security posture and implement the recommended mitigation strategies

- Architectural reviews and analysis assessments are also available
Cyber Security Evaluation Tool (CSET)

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

CSET Download:
us-cert.gov/control_systems/csetdownload.html
Component Questions
Analysis Screen
Hardcopy Reports
Resource Library

This library of cyber security standards, reports, and templates are provided for your convenience. Additionally, there are several cyber security guides and white papers to assist you in building a robust cyber security program.