U.S. DEPARTMENT OF ENERGY

Department of Energy (DOE) Office of the Chief Information Officer (OCIO) Brief

Amy Hamilton

Senior Advisor for National Cybersecurity Policy and Programs

MOSAICS Industry Day
May 18-19, 2021

DOE Control Systems Working Group (CSWG)

Vision

Develop a strategy and amplification guidance to strengthen the DOE cybersecurity posture and support enhanced operational visibility of Control System devices and improved stewardship of Control System-associated data.

Objectives

1. Provide Asset Inventory;
2. Address Common Vulnerabilities and Attack Techniques;
3. Provide Control Systems Instrumentation Guidance;
4. Provide Configuration Recommendations; and
5. Recommend Improvements to Ongoing Processes and Systems.

With **60+ DOE organizations** involved in the CSWG across Program Offices, Laboratories, and Agencies:

Program Offices	Staff Offices	Agencies
• **CESER** – Office of Cybersecurity, Energy Security, and Emergency Response • **ERRE** – Energy Efficiency & Renewable Energy • **EM** – Office of Environmental Management	• **IM** – Office of the Chief Information Officer • **IN** – Office of Intelligence & Counterintelligence • **AU** – Office of Environmental, Health, Safety, and Security	• **NNSA** – National Nuclear Security Administration

DISTRO A: Approved for Public Release. Distribution is unlimited.

Training Opportunities

DOE Organization	Training Details
Los Alamos National Laboratory (LANL)	**Cyber Fire:** • Bi-annual DOE Cyber Fire offers a suite of cybersecurity training events for beginner to expert cyber incident analysts. • The training is a week-long event featuring two days of classes, two days of hands-on exercises, and a final day of briefings.
Idaho National Laboratory (INL) Consequence-Driven Cyber-Information Engineering (CCE)	**ACCELERATE Training:** • Offers critical infrastructure companies a self-guided approach to conducting their own CCE effort. • ACCELERATE is a two-day training on CCE concepts and methodology, plus a detailed guide and templates participants can use to facilitate a CCE evaluation within their organization.
SANS Training	**SAN Courses:** • ICS/SCADA Security Essentials – Fundamentals to industrial control systems (ICS) or information technology (IT) work. • ICS456-Essentials for North America Electric Reliability Corporation (NERC) Critical Infrastructure Protection – Focuses on identifying and categorizing Bulk Electric System (BES) cyber systems. • ICS515-ICS Active defense and Incident Response – Focuses on threat hunting in ICS and an active defensive approach. • ICS612-ICS Cyber Security In-Depth – Hands on lab meant for practitioners in the field

DISTRO A: Approved for Public Release. Distribution is unlimited.

Use Case Studies

DOE Organization	Use Case Study Details
Idaho National Laboratory (INL) Consequence-Driven Cyber-Information Engineering (CCE)	**"Stinky Cheese Company":** • Fictional case study where the CCE methodology was applied to identify worst-case functional impacts and determine High Consequence Events (HCEs). • Examined potential negative production/business impacts of cyber-enabled sabotage against a fictional entity.
Pacific Northwest National Laboratory (PNNL)	**Tenable OT & IoT Risk Reduction:** • Conducted an assessment to determine which operational technology (OT) / Internet of things (IoT) devices to focus on and which tools are needed to implement at PNNL for risk reduction. The assessment results found 6,800 OT and 1,100 IoT assets. • Several scenarios were built in order to identify and assess existing areas of risk. Risk mitigation recommendations can be developed to address the existing risks found.
DOE Office of the Chief Information Officer (OCIO) Supply Chain Risk Management (SCRM)	**SCRM Strategy:** • DOE OCIO developed a SCRM strategy for DOE, which covers establishing governance, cross-program office integration, and a SCRM program designed to drive consistency in identifying, treating, and mitigating supply chain risks while adapting to evolving threats. • In response to several recent high-profile supply chain breaches, the OCIO is focused on protecting supplier products and services for Information and Communication Technology (ICT) devices.

DISTRO A: Approved for Public Release. Distribution is unlimited.