Agency Priority Goal Action Plan

Strengthen Cybersecurity Capabilities

Goal Leader:

Karen S. Evans - Cybersecurity, Energy Security, and Emergency Response (CESER) Assistant Secretary

Theme(s): Energy

Performance.gov

Fiscal Year 2019, Quarter 4

Overview

Goal Statement

- Strengthen energy sector cybersecurity capabilities.
  - By September 30, 2019, DOE will complete the operational technology data analysis from at least three utilities and develop a recommendation for deployment of the operational technology cyber security approach to utility operators nation-wide.

Challenge

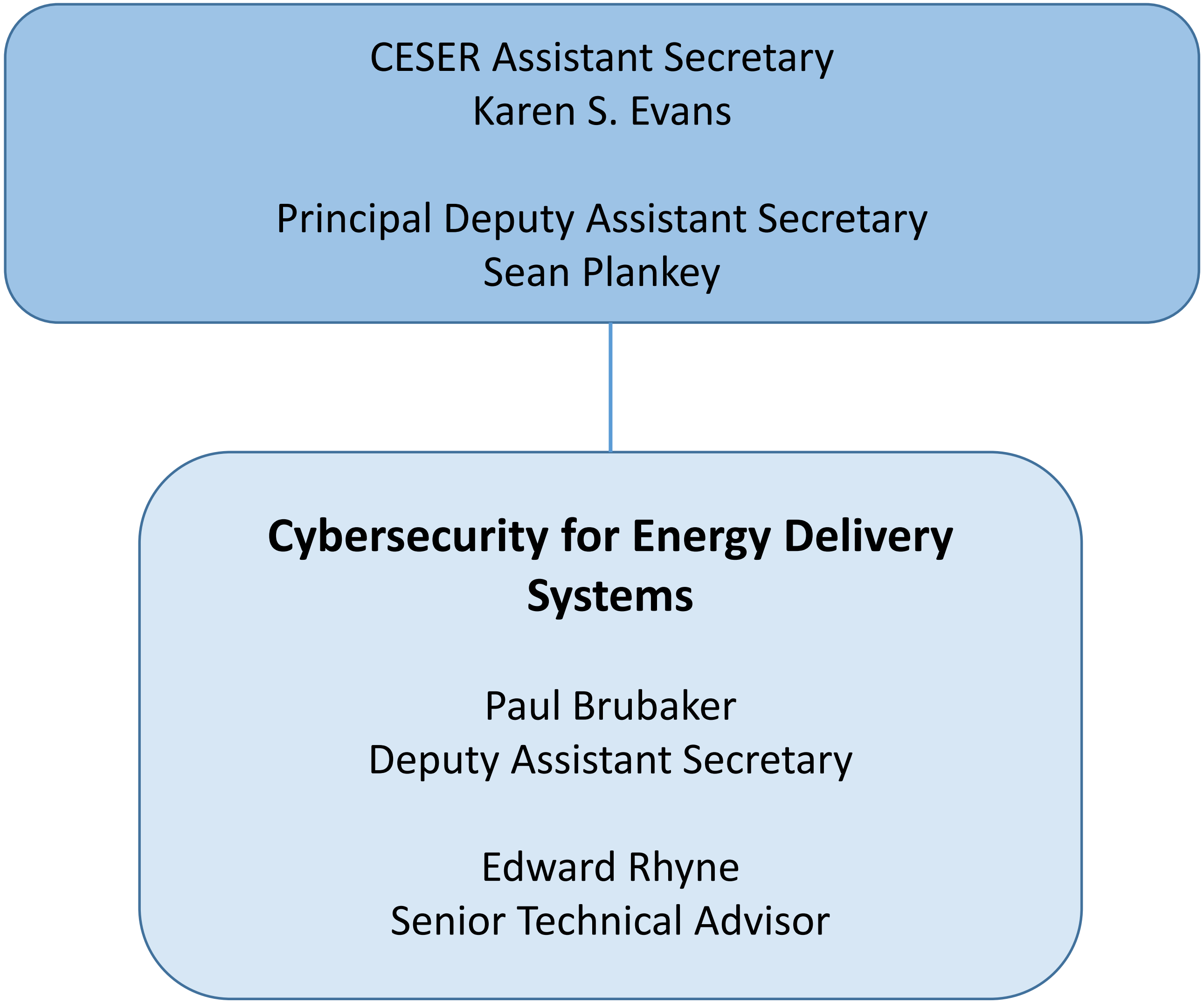
- Control systems at energy utilities have become a key target for cyberattacks. Attacks have become more sophisticated and coordinated, making it difficult for utilities to know if their systems have been penetrated and are at risk.
- Identifying risks and detecting attacks on operational technology (OT) systems requires utilities to know where to look—and what to look for—in complex operating environments.
- The lack of visibility in OT networks today creates a blind spot in critical energy infrastructure, leaving operators unable to adequately detect, identify, and block malicious activity.

Overview

Opportunity

- In contrast with their IT systems, few utilities have robust capabilities to collect data from their OT networks, analyze it effectively, and detect sophisticated attacks in real time.
- Cybersecurity for the Operational Technology Environment (CyOTE^{TM}) pilots with utilities are designing an industry-led collaborative approach—one that leverages advanced commercial tools in utility environments and elicits expert analysis from the U.S. intelligence community and DOE national laboratories—to deliver actionable intelligence to help utilities identify and mitigate OT threats.
- Pilots will develop an initial CyOTE^{TM} operational capability for OT sensing, data sharing, and analysis and recommend risk-based approach to expand this capability to utilities nation-wide.

Leadership



CESER Assistant Secretary
Karen S. Evans

Principal Deputy Assistant Secretary
Sean Plankey

Cybersecurity for Energy Delivery Systems

Paul Brubaker
Deputy Assistant Secretary

Edward Rhyne
Senior Technical Advisor

Goal Structure & Strategies

Long-Term Vision for CyOTE^{TM} Capability

Create an *industry-wide* capability to:

- Share near-real-time OT network data and leverage U.S. intelligence capabilities to detect sophisticated cyber threats.
- Deliver actionable information to utilities to better protect U.S. electric power infrastructure against cyber attacks.

Given the complexity of the challenge, DOE launched a pilot to develop, test, and validate an OT data sharing and analysis solution that will scale into a larger, industry-wide effort.

Goal Structure & Strategies

CyOTE^{TM} Pilot Goal - PILOT AN APPROACH TO OT DATA SHARING AND INTELLIGENCE ANALYSIS

1. Develop, test, and validate a process to:
    - Identify high-risk OT attack scenarios, monitoring points, and monitoring tools
    - Securely share OT network data between partner utilities and the government
    - Develop OT-centric analytics that leverage U.S. Intelligence insights to detect sophisticated cyber threats
2. Evaluate technical feasibility to expand CyOTE^{TM} pilot solution to additional priority utilities using a risk-based approach
3. Recommend an approach for a sustained nation-wide CyOTE^{TM} program that balances government investment and private investment from participating utilities

Goal Structure & Strategies

CyOTE^{TM} Pilot Objectives and Approach

- Produce a **risk-based methodology for collecting and sharing OT data** for generation, transmission, and distribution networks

- **Utilize advanced commercial sensors,** and **share and analyze OT data streams** using advanced OT analytics and Intelligence Community tools and insights.

- Determine **whether CyOTE^{TM} analysis can provide timely, actionable information to help utilities protect their networks** against sophisticated attacks.

- Identify and **recommend a methodology to expand CyOTE^{TM}** analysis into a rapid, industry-wide capability

Goal Structure & Strategies

Measuring Pilot Effectiveness - A successful pilot will result in:

- Secure OT network data sharing and Idaho National Laboratory (INL)/intelligence analysis
- Assessment of the value added from CyOTE^{TM} analysis at each network location
- Recommendations of sensor requirements, locations, and data formats for CyOTE^{TM} expansion.

Summary of Progress – Final

- The CyOTE^{TM} pilot has executed data protection agreements with partner utilities.
- Acquired OT data from key network tap points in partner utility infrastructures.
- Analyzed three partner utility's OT data and convened meetings with each to discuss results and provide context for further refinement of the analysis process.
- Identified commercial anonymization tools and completed testing. Determined that a commercial solution will not meet our requirements for protecting Personally Identifiable Information as well as Entity Identifiable Information (EII) and Device Identifiable Information (DII).
- Continued development for integration of OT context and OT protocol parsing to ensure analysis is appropriate for capture environments based on initial data set analysis.
- Utilized the MITRE Adversarial Tactics Techniques & Common Knowledge (ATT&CK™) framework as a method of identifying potential threat tactics, techniques and procedures (TTP's) that may be present in US electric utility OT network data. Selected a subset of TTP's for analysis based on the data provided by the participating utilities, coverage of the attack lifecycle, and impact to the power sector. Prioritization of threat actor TTP's based upon:
  - Analysis of threat reporting regarding current OT cyber activity
  - Analysis of known actor capabilities and indicators of future capability growth
  - Interviews with leading OT cyber first responders to understand patterns they see in current incident response
  - Identification of areas of the OT network (and related TTP's) which have high potential value but may be difficult to monitor effectively
- Created tools to ensure next generation analytics framework and data analytics processes are aligned with strategic data captures.

Statement of Goal Achievement and Next Steps

Goal Statement

- Strengthen energy sector cybersecurity capabilities.
  - By September 30, 2019, DOE will complete the operational technology data analysis from at least three utilities and develop a recommendation for deployment of the operational technology cyber security approach to utility operators nation-wide. **Met**

APG Status: **Achieved**

Next Steps:

- Does DOE have an FY 2020-2021 APG in this topic area? **Yes**

Key Milestones

Milestone Summary				
Key Milestone	Milestone Due Date	Milestone Status	Owner	Comments
Acquire OT data from pilot participants	November 30, 2018	Complete (April 2019)	GC/CESER	Data agreements for three utilities have been signed and data is being received.
Complete the analysis of utility OT data	March 31, 2019	Complete (July 2019)	INL	The OT data analysis is a new frontier that is being explored with multiple technological challenges, e.g. managing data volume and developing OT-centric protocols. Delay in data acquisition and analysis will impact this milestone.
Develop the methodology to operationalize OT threat analysis by exception	July 31, 2019	Complete (July 2019)	INL	Determined the network baseline and operational context needed to identify the OT network exceptions.
Complete the pilot and develop a recommendation for an industry-wide approach	September 30, 2019	Complete (August 9, 2019)	INL	Operationalized the approach for industry-wide application and obtain industry buy-in for implementation. Milestone completed ahead of schedule.