Improving Grid Resilience

November 12, 2013

Mike Smith
Senior Cyber Policy Advisor to the Assistant Secretary
Office of Electricity Delivery and Energy Reliability
Department of Energy
Overview

• President Obama in his 2013 State of the Union Address:
  – “America must also face the rapidly growing threat from cyber-attacks… our enemies are also seeking the ability to sabotage our power grid, our financial institutions, our air traffic control systems….we cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy.”

• Three areas of focus for DOE:
  – Cybersecurity in the energy sector
  – Protecting the DOE complex
  – Bolstering USG capabilities
Implementation of E.O. 13636 and PPD-21

• Executive Order 13636 on Improving Critical Infrastructure Cybersecurity

• Presidential Policy Directive 21 on Critical Infrastructure Security and Resilience (PPD-21)

• The White House directed DHS to establish an Integrated Task Force to facilitate implementation
  – Update the National Infrastructure Protection Plan
  – Increase information sharing
  – Develop a Cybersecurity Framework (standards, practices, and procedures)
August 15, 2012 Saudi Aramco computers were infected with the “Shamoon” malware

- Attack erased data on tens of thousands of computers
- Aramco shut down its corporate network (email, internet) for over a week to stop the spread of the virus

Segregation of IT and OT prevented the virus from compromising Aramco’s oil production

Source: http://www.infosecurity-magazine.com/view/29750/shamoon-was-an-external-attack-on-saudi-oil-production/
Energy Sector Cybersecurity

Energy Delivery Control Systems

- Energy delivery control systems (EDS) must be able to survive a cyber incident while sustaining critical functions
- Power systems must operate 24/7 with high reliability and high availability, no down time for patching/upgrades
- The modern grid contains a mixture of legacy and modernized components and controls
- EDS components may not have enough computing resources (e.g., memory, CPU, communication bandwidth) to support the addition of cybersecurity capabilities that are not tailored to the energy delivery system operational environment
- Energy delivery control system components are widely dispersed over wide geographical regions, and located in publicly accessible areas where they are subject to physical tampering
- Real-time operations are imperative, latency is unacceptable
- Real-time emergency response capability is mandatory

Business IT Systems
Electricity Subsector Risk Management Process

DOE created the electricity subsector Risk Management Process in conjunction with utilities, regulators, and other Federal stakeholders.

The successful application of this process will result in the ability of an Electricity Subsector organization to:

- Effectively and efficiently implement a cybersecurity Risk Management Process (RMP) across the whole organization;
- Establish the organizational tolerance for risk and communicate it throughout the organization, including guidance on how risk tolerance impacts ongoing decision making;
- Prioritize and allocate resources for managing cybersecurity risk;
- Create an organizational climate in which cybersecurity risk is considered within the context of the mission and business objectives of the organization; and
- Improve the understanding of cybersecurity risk and how this risk potentially impacts the mission and business success of the organization.
Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)

- Measures the degree to which cybersecurity processes are institutionalized
  - Institutionalized processes are more likely to be retained during times of stress

- Objectives:
  - Strengthen cybersecurity capabilities
  - Enable consistent evaluation and benchmarking of cybersecurity capabilities
  - Share knowledge and best practices
  - Enable prioritized actions and cybersecurity investments
Cybersecurity Risk Information Sharing Program (CRISP)

Overview - Combines software tools, analytical hardware and software, and analytical expertise – including private sector industry experience - to understand and mitigate the threats focused on the nation’s energy infrastructure

Purpose - Collaborate with private electric sector partners to:

• Facilitate the timely sharing of unclassified and classified threat information
• Develop situational awareness tools
• Enhance the sector’s ability to identify, prioritize, and coordinate the protection of their critical infrastructure and key resources

Way Forward - Complete FY13 pilot with four entities and prepare for the addition of 20 new entities in FY14
Goals:

• To have near real-time, bi-directional, machine speed information sharing of different threat observables between public and private sectors

• To create an energy sector common operational picture
Incident Management

• DOE is leading the development of an Energy Sector Cyber Incident Management Capability
  – Processes for incident management
  – Sharing of information exchange protocols
  – Developing technology requirements

• DOE is working with DHS and industry on a series of exercises:
  – Poison Apple in August 2013
  – NERC GridEx in November 2013
The Roadmap addresses the Energy sector’s goals and challenges in improving its cybersecurity posture.

The roadmap is organized by milestones in five key strategies:

- Build a culture of security
- Assess and monitor risk
- Develop and implement new protective measures to reduce risk
- Manage incidents
- Sustain security improvements

The vision of the cybersecurity roadmap is:

- By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.
CEDS Program Structure

Higher Risk, Longer Term Projects
→ Core NSTB Program
→ Frontier Research
→ Academia Projects
→ Minimum Cost Share

Medium Risk, Mid Term Projects
→ National Laboratory Led Projects
→ Lower Cost Share

Lower Risk, Shorter Term Projects
→ Industry Led Projects
→ Higher Cost Share

Path to Commercialization

Partnering

Core & Frontier (NSTB)
• Argonne National Laboratory
• Idaho National Laboratory
• Oak Ridge National Laboratory
• Los Alamos National Laboratory
• Lawrence Berkeley National Laboratory
• Pacific Northwest National Laboratory
• Sandia National Laboratory

Academia – Led
• Trustworthy Cyber Infrastructure for the Power Grid (TCIPG)
  – Cornell University
  – Dartmouth College
  – UC-Davis
  – University of Illinois
  – Washington State University
• SEI at Carnegie Mellon

Laboratory – Led
• Idaho National Laboratory
• Oak Ridge National Laboratory
• Pacific Northwest National Laboratory

Industry – Led
• Applied Communication Services
• Grid Protection Alliance
• Honeywell
• Schweitzer Engineering Laboratories, Inc.
• Siemens Infrastructure & Cities, Energy Automation
• Sypris
Questions?

Mike Smith
Senior Cyber Policy Advisor to the Assistant Secretary
Office of Electricity Delivery and Energy Reliability
Department of Energy
Email: Mike.Smith2@hq.doe.gov
Phone: 202-586-8710