RSA Conference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

Session ID: PNG-F01

Cybersecurity Risk Information Sharing Program (CRISP): Bi-Directional Trust

Michael E. Smith
Senior Cyber Policy Advisor to the Assistant Secretary, Office of Electricity Delivery and Energy Reliability, U.S. Department of Energy

#RSAC

How serious is the threat?

- Sophisticated, patient actors have gained direct access to control systems
  - Presence goes undetected for years
- More ICS devices are being connected to the internet, intentionally and unintentionally
- Search engines are enabling the discovery and identification of internet facing devices
  - Scanning and cataloguing of devices with known vulnerabilities is ongoing

Objectives

- Increase awareness of the Cybersecurity Risk Information Sharing Program (CRISP) and its robust new model of public-private partnership
- Recognize the challenges posed by current U.S. laws and policies in getting CRISP up and running
- Examine how we jointly addressed these challenges
- Persuade you to pursue similar partnerships

What is the impact of CRISP?

- One of a kind partnership
- Pushing the boundaries of information sharing
- Current participants provide electric power to 60,107,604 customers - 45.68% of the continental U.S. total

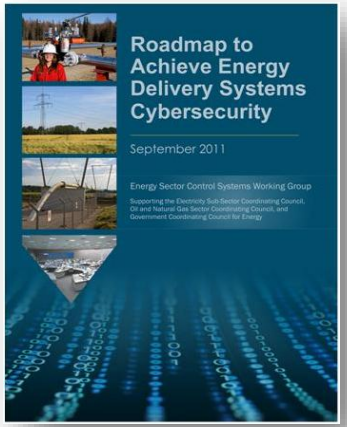
The Foundation of Trust

- Achieving bi-directional trust
- The authorities and policies that define our relationship
- The programs and events that sustain our relationship

The Energy Sector Roadmap

- Provides strategic framework to:
  - Align activities to sector needs
  - Coordinate public and private programs
  - Stimulate investments in ICS security

www.controlsystemsroadmap.net

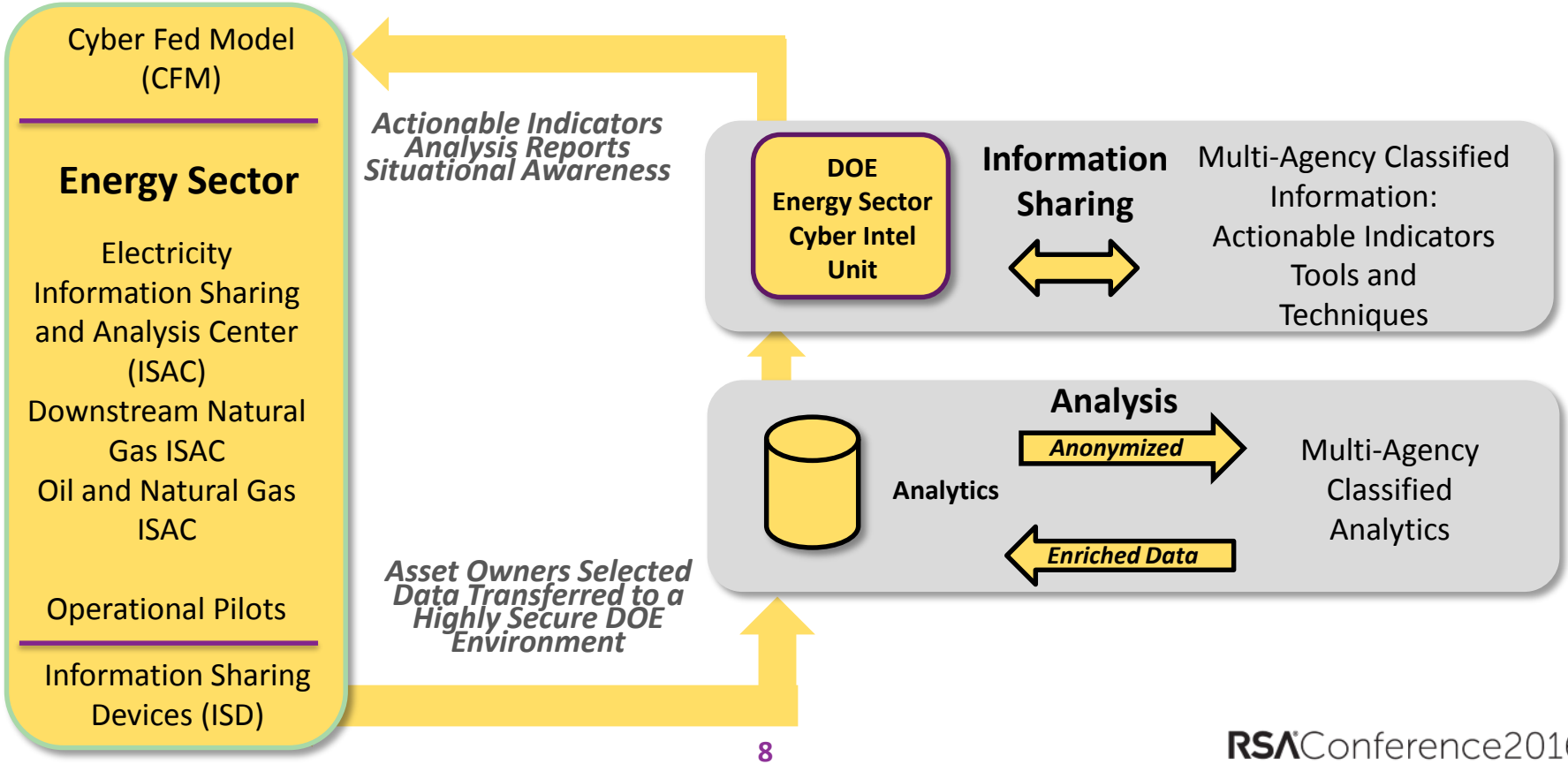


- Build a Culture of Security
- Assess and Monitor Risk
- Develop and Implement New Protective Measures to Reduce Risk
- Manage Incidents
- Sustain Security Improvements

Participants

- The government
  - Department of Energy
  - And the rest of the government
- Industry
  - Energy Sector
    - Information Sharing and Analysis Centers
    - Owners and operators
  - Cybersecurity service providers

Architecture



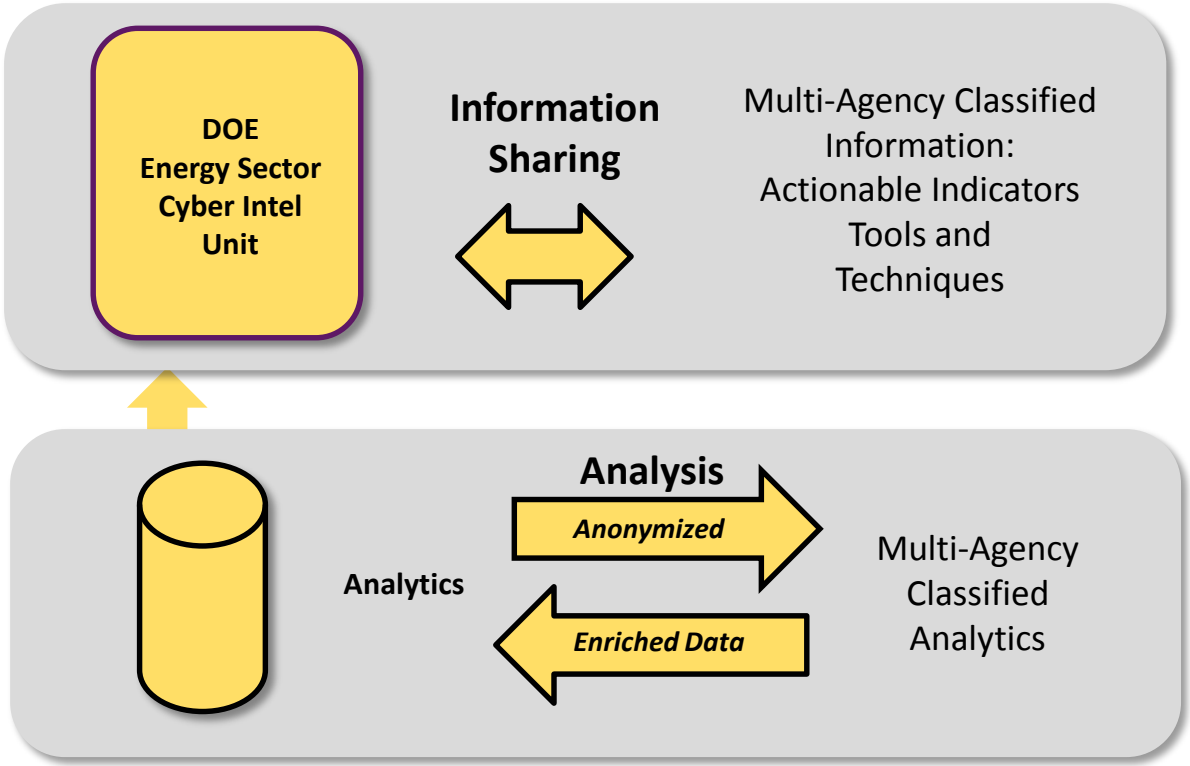
Five Year Plan – Mission and Vision

- **Mission:** By utilizing advanced technologies and innovative analytical capabilities:
  - establish and maintain effective collaboration with energy sector partners through robust **bi-directional information sharing**
  - provide energy sector partners with targeted, **actionable information** to enable requirement setting, detection, prevention, mitigation, and rapid response to emerging threats
- **Vision**: By 2019, an enduring, trusted **bi-directional** information sharing partnership between the Department of Energy and its energy sector partners significantly enhances the security of energy sector infrastructure systems and improves the U.S. Government's **near real-time situational awareness.**

Five Year Plan - Goals

- Efficient and effective decision making is a sector challenge
- DOE will focus on three strategic goals to address this challenge:
  - **Data enrichment**
  - **Analytic platform**
  - **Operational pilots**

Strategic Goal 1: Data Enrichment



#RSAC
RSAConference2016

Strategic Goal 2: Analytic Platform

- Platform is key to managing increasing data diversity and must:
  - provide both industry and government with **near real-time actionable threat information;**
  - **facilitate collaborative analysis**; and
  - **deliver the insight** required for crucial risk management decisions.
- The platform will also:
  - shape and evaluate sensor technologies;
  - identify capability gaps; and
  - enhance and help correlate data

Strategic Goal 3: Operational Pilots

- **Investigate technologies and capabilities** that improve CRISP
- Ensure **operational activities align** with industry priorities
- **Collaborate** with DHS, the ISACs, energy sector, and cybersecurity vendors to:
  - identify and validate **pilot targeted capabilities**
  - **review proposals**, and select pilot awardees
  - conduct subsequent **evaluation** and assessment

1st Operational Pilot – Norse-FireEye

- Norse Corporation

- FireEye

Year One Results

- **Direct results**:
  - capability (architectural, technology, and process) improvements and/or gaps identified and incorporated by CRISP, Norse, FireEye and the volunteer participants;
  - volunteer participants choose to remain in CRISP after the pilot ends
- **Indirect results**:
  - raising energy sector awareness of the range of best in class commercially available cybersecurity capabilities while also;
  - raising the cybersecurity industry awareness of the unique concerns, challenges, and threats faced by the energy sector

Next Operational Pilots – ICS Focused

- Adding two new national labs
- Fully implementing machine-to-machine sharing
- Identifying and employing ICS situational awareness capabilities

http://www.grants.gov/

Apply

- Develop your own trusted information sharing relationships
- Actively participate in U.S. Government information sharing programs
- Question existing information sharing models and advocate for improvements

Summary – We can't wait…

- CRISP represents a ground-breaking new model of public-private partnership
- U.S. laws and policies have historically not kept pace with the current cyber threat landscape nor with this type of aggressive partnership
- DOE and its energy sector partners jointly decided that we needed to act now
- I encourage all of you to do the same

Questions?

Mike Smith
202-586-8710
Michael.smith2@hq.doe.gov
Cybersecurity for Energy Delivery Systems Program
Website: http://energy.gov/oe/services/technology-development/energy-delivery-systems-cybersecurity