U.S. DEPARTMENT OF ENERGY
ENERGY SECTOR CYBERSECURITY OVERVIEW

November 12, 2012

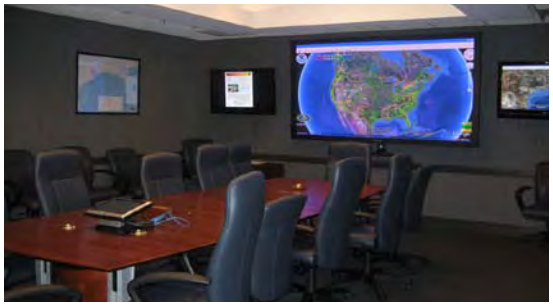
NASEO

National Shift

From Protection to Resilience

ISER Response: from site focused to system focused

- **Emergency Preparedness, Response, and Restoration**
- **Analysis and Situational Awareness**
- **Physical and Cyber System Assurance**
- **Global Energy Assurance**



Collaboration

DOE is the Energy Sector-Specific Agency

National Infrastructure Protection Plan:

- Created the framework for public-private partnerships across the nation's critical sectors and established DOE as the energy sector-specific agency .
- Electricity and Oil and Natural Gas Sector Coordinating Councils share information with the Energy Government Coordinating Council, an interagency effort.
- **Energy Sector-Specific Plan** – Defines the goals and activities of the sector as a whole, written by ISER in collaboration with our public and private sector partners.

National Response Framework:

- Established the guiding principles that enable all response partners to prepare for and provide a unified national response to disasters and emergencies.
- **Emergency Support Function #12 – Energy** – Designated under the NRF, and intended to allow the Department of Energy, as well as a variety of other relevant government agencies, to quickly and effectively respond to and recover from severe damage to the nation's energy infrastructure.
  - ISER executes this responsibility on behalf of the Department.

Energy Sector

Includes Electricity, Oil and Natural Gas

Segments of the Energy Sector

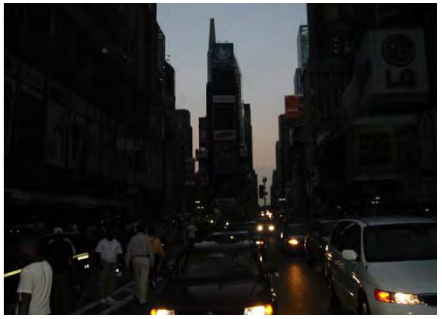
Electricity	Petroleum	Natural Gas
• Generation – Fossil Fuel Power Plants » Coal » Natural Gas » Oil – Nuclear Power Plants[a] – Hydroelectric Dams[a] – Renewable Energy • Transmission – Substations – Lines – Control Centers • Distribution – Substations – Lines – Control Centers • Control Systems • Electricity Markets	• Crude Oil – Onshore Fields – Offshore Fields – Terminals – Transport (pipelines)[a] – Storage • Petroleum Processing Facilities – Refineries – Terminals – Transport (pipelines)[a] – Storage – Control Systems – Petroleum Markets	• Production – Onshore Fields – Offshore Fields • Processing • Transport (pipelines)[a] • Distribution (pipelines)[a] • Storage[b] • Liquefied Natural Gas Facilities[b] • Control Systems • Gas Markets

[a] Hydroelectric dams, nuclear facilities, rail, and pipeline transportation are covered in other SSPs.

[b] Certain infrastructure of this asset type are regulated by the Chemical Facility Anti-Terrorism Standards (CFATS). The final tiering of the facilities covered by the CFATS was not completed at the time of this report.

2003 Northeast Blackout

- The blackout affected as many as 50 million people in the United States and Canada, as well as a wide range of vital services and commerce.
- The lost productivity and revenue have been estimated in the billions of dollars.
- A series of power plants and transmission lines went offline beginning at about noon eastern daylight time because of instability in the transmission system in three states. The loss of these plants and transmission lines led to greater instability in the regional power transmission system, which—4 hours later—resulted in a rapid cascade of additional plant and transmission line outages and widespread power outages throughout the northeast.
- A combination of causes and contributing factors led to the blackout including failure to identify emergency conditions and communicate status to neighboring systems, inadequate vegetation management, inadequate operator training and others.
- Examples of DOE actions in addressing the Blackout include:
  - Coordinating with DHS and the Federal Energy Regulatory Commission (FERC) in gathering information and responding to the Blackout.
  - Coordinating with states through its state communications program and helping them enact measures to respond to the Blackout.
  - Monitoring activity on the electric grid with NERC.
  - Coordinating fuel status data for backup power supplies that were essential to Blackout recovery efforts.
  - Tracking petroleum refinery status and shutdowns.
  - After the event: U.S. Secretary Energy and Canada's Minister of Natural Resources chaired a Joint Task Force to investigate the outage and determine its causes and why was not contained and to develop recommendations to reduce possibility of future outages.



Electricity Subsector as an Example

Guidance, Policy, Regulation

- Electricity Sector organizations (utilities, generator owners, transmission owners, etc.) face a variety of regulation, guidance, and policies from local, state, and federal stakeholders.

- Various types of guidance (safety, personnel, operations, security) may influence or dictate cybersecurity requirements.

- This guidance is sometimes conflicting, broad, or misaligned with business mission and operations. This in turn can lead to the inconsistent implementation of cybersecurity both within and between electricity sector organizations.

- Thus, clearly identifying, scoping, and incorporating these requirements is an important component to effectively managing cybersecurity risk.

Electricity Subsector Policy

Stakeholders

- There is a large number of diverse stakeholders across the Electricity Sector with differing cybersecurity expectations and objectives. Additionally, their understanding of industry operations and cybersecurity varies and is framed by their own organization's mission.

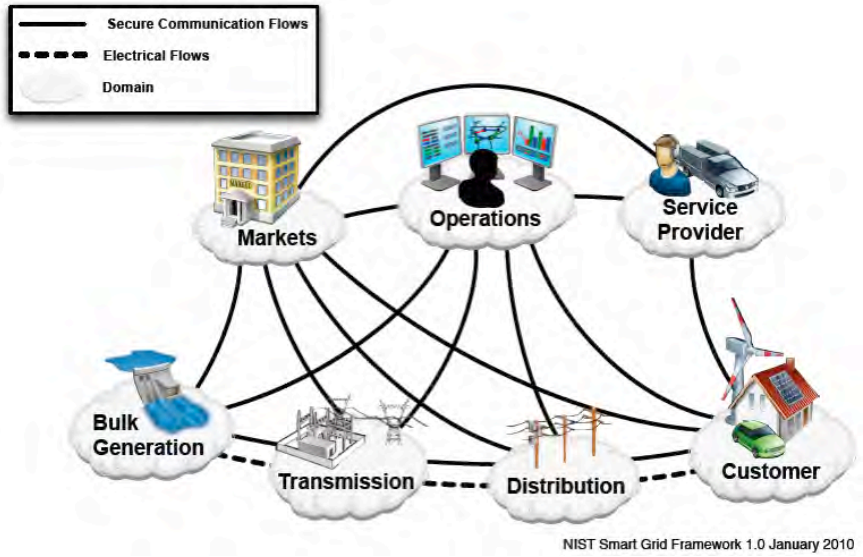
  - Federal regulators(FERC, NERC, NRC)

  - Federal stakeholders (DOE, NIST, DHS, DOD, Congress)

  - State and provincial regulators and stakeholders (PUCs, State Energy Offices)

Changing Operational Landscape

- Increasing use of digital technologies is changing the cyber landscape of the industry
  - Smart meters
  - IT and ICS merging
  - Sensing and monitoring
  - Dynamic pricing
- The increase in connectivity across traditionally segmented operations has several impacts to the cybersecurity risk of the organization
  - Increased vulnerabilities
  - Greater impact across the organization
  - Introduction of third party risk
  - Conflicting requirements
- The result is a potential increase in risk to the organization's business mission and operations



NIST Smart Grid Framework 1.0 January 2010

Changing Threat Landscape

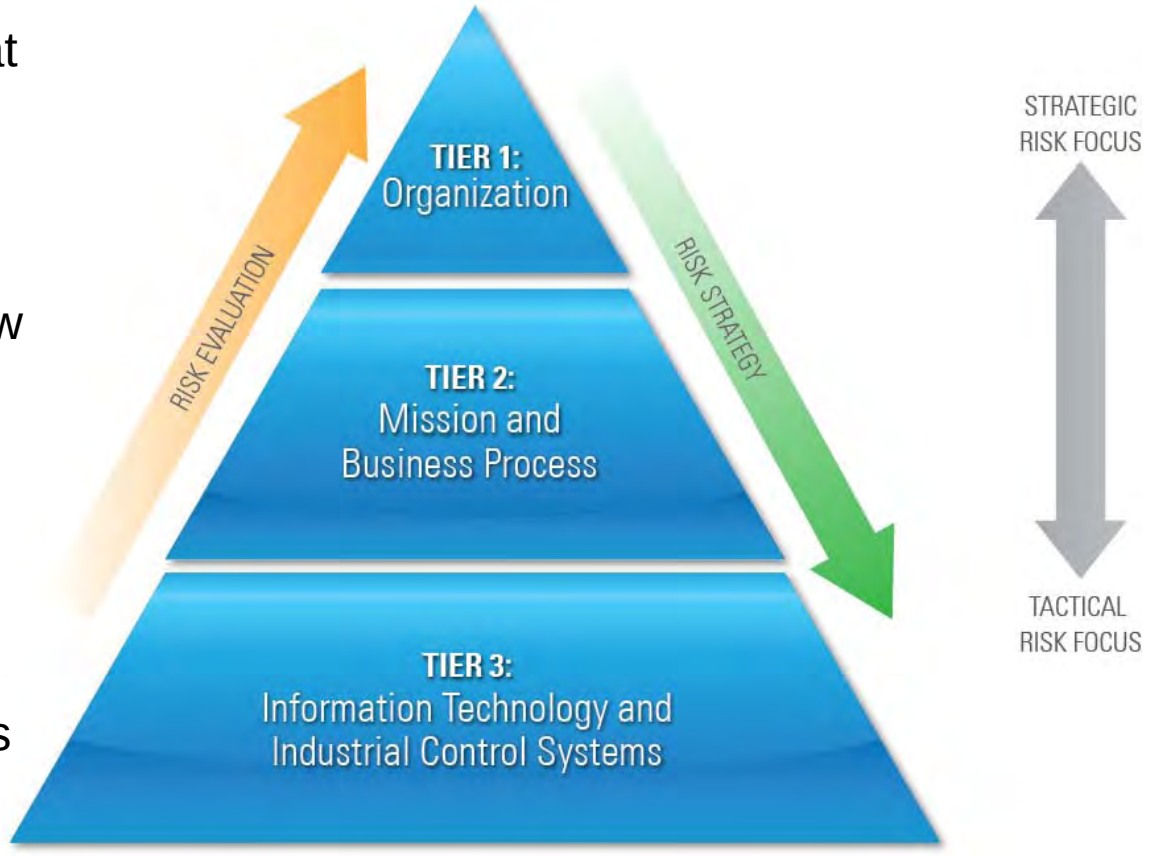
- Increasing trend of cyber attacks targeted at energy and pipeline infrastructure around the world
  - Malicious and destructive
  - Unpredictable
  - Increasing capabilities and effectiveness
- The result is a cumulative increase in risk to the organization's business mission and operations

The Need for a Harmonized Risk Management Process

- The Energy Sector is diverse and the jurisdictions and environments they operate in varies significantly across the industry
  - -Type: Generation, transmission, distribution, retail, and energy service providers
  - - Jurisdiction: federal, state, provincial, municipal
  - - Environment: urban, suburban, rural
- A “one size” fits all standard requirement is not practical
- Need to establish a consistent, repeatable, and adaptable process for risk management across the entire electricity sector
- Based on the NIST SP 800-39: Managing Information Security Risk
- The process:
  - - Adaptable to meet individual organizational requirements
  - - Recognizes organizational constraints (resources, personnel, policy)
  - - Allows resource allocation based on risk management principles
  - - Identifies ownership of risk within the organization

Risk Management Model

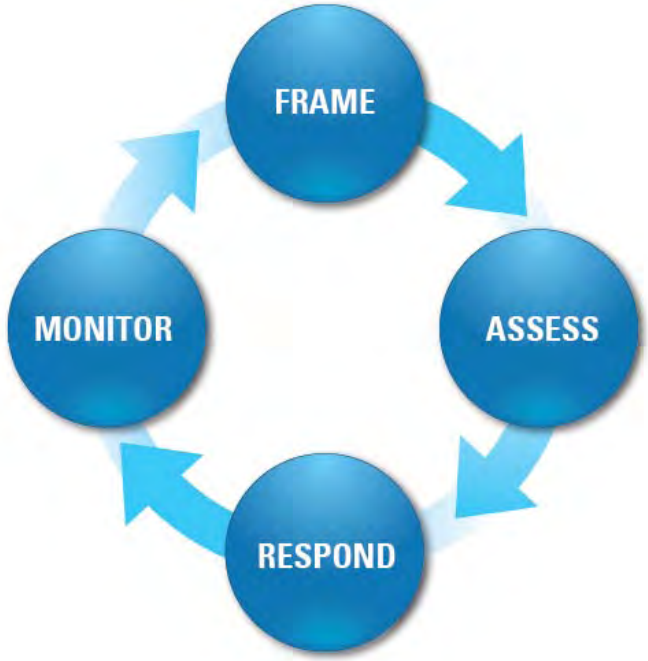
- The risk management model is a three-tiered structure that provides a comprehensive view of an Electricity Sector organization
- It provides a structure for how cybersecurity risk management activities are undertaken across an organization
- Strategy is communicated down through the organization, risk evaluations are communicated up



Risk Management Cycle

- The risk management cycle provides four elements that structure an organization's approach to cybersecurity risk management

- The risk management cycle is not static but a continuous process, constantly re-informed by the changing risk landscape as well as by organizational priorities and functional changes



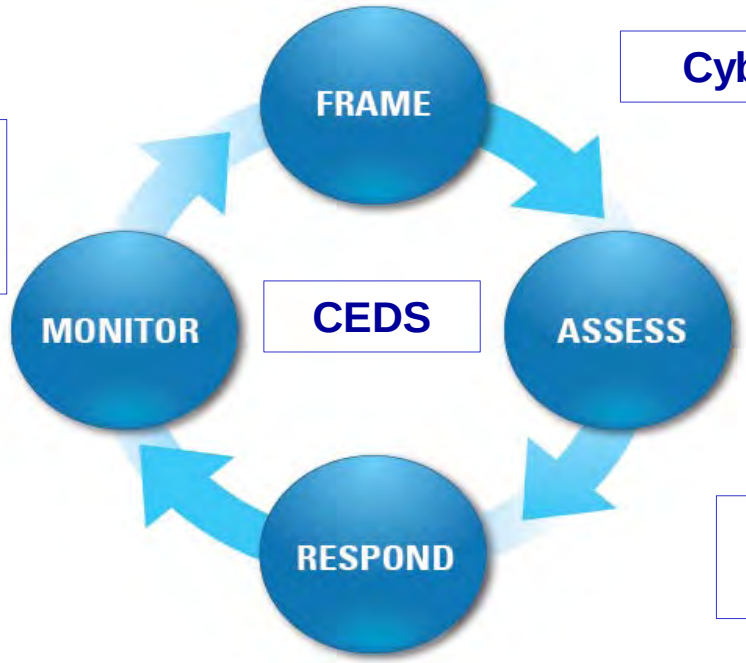
Federal Cybersecurity Efforts

Cyber Threat Environment

DHS NCCIC

Cyber Taxonomy

Sector Specific Agency – Coordination and Networking



Electricity Sector Cybersecurity Capability Maturity Model

ES-ISAC

CEDS

DHS CSET Tool

NESCO Tactical Analysis Center

Secure Power Systems Specialist Project

EAGLE I

NCIRP

Local FBI Field Office

Energy Sector Incident Management

DHS ICS-CERT

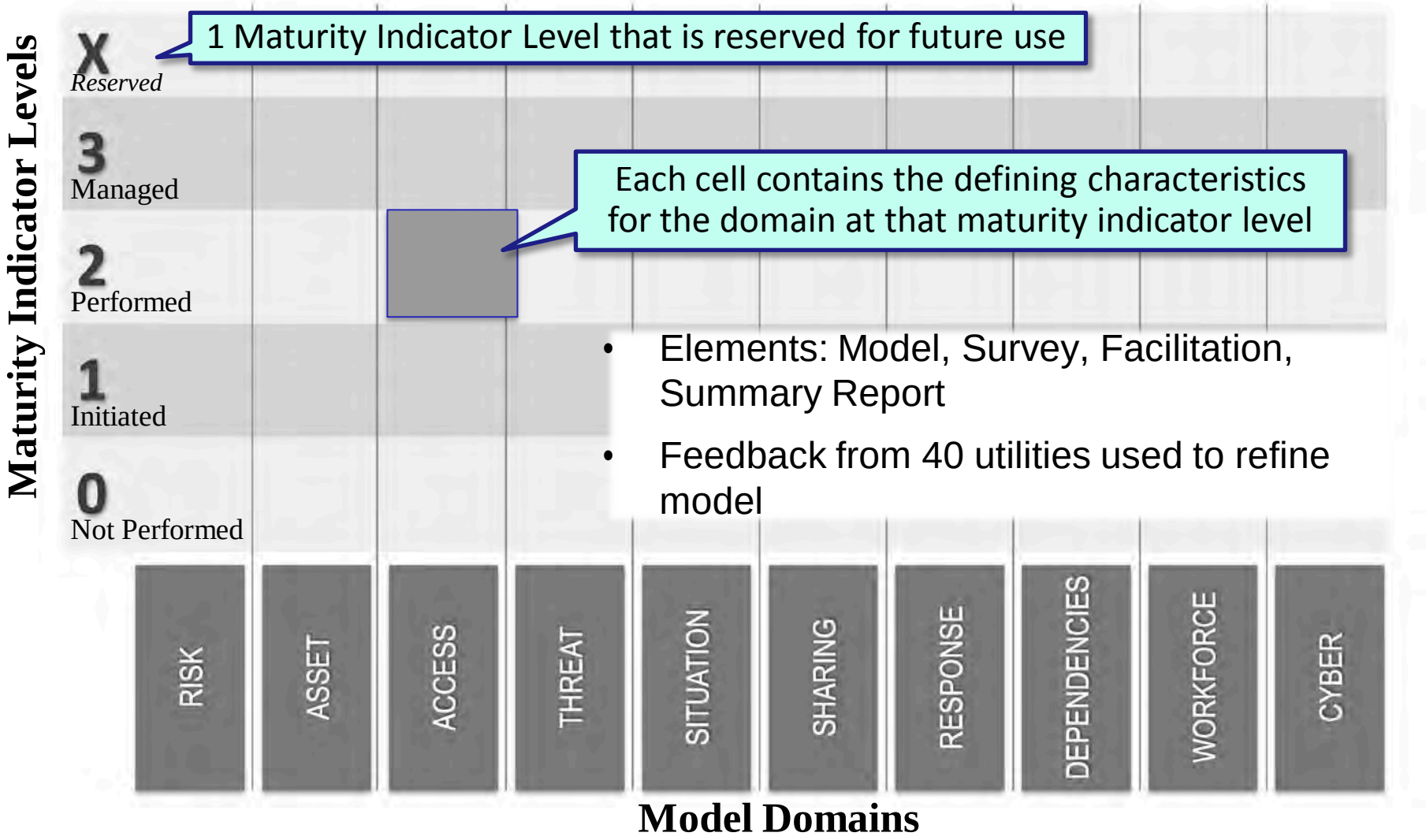
ES-C2M2 Background & Overview

- Challenge: Develop capabilities to manage dynamic threats and understand cybersecurity posture of the grid
- Approach: Develop a maturity model and self-evaluation survey to develop and measure cybersecurity capabilities
- Results: A scalable, sector-specific model created in partnership with industry

ES-C2M2 Objectives

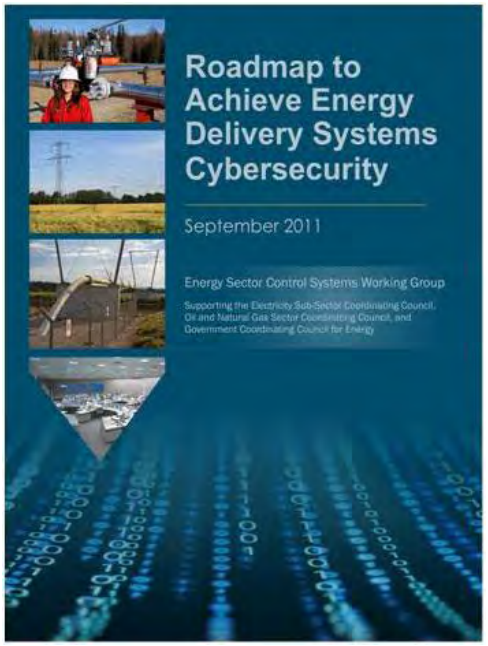
- Strengthen cybersecurity capabilities
- Enable consistent evaluation and benchmarking of cybersecurity capabilities
- Share knowledge and best practices
- Enable prioritized actions and cybersecurity investments

ES-C2M2 Overview



Roadmap

Framework for Collaboration



- *Energy Sector's* synthesis of critical control system security challenges, R&D needs, and implementation milestones
- Provides strategic framework to
  - align activities to sector needs
  - coordinate public and private programs
  - stimulate investments in control systems security

Roadmap Vision

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

For more information go to: www.controlsystemsroadmap.net