Agenda

- Background
- Use of Existing Tools: C2M2 Case Study
- Next Steps for the Energy Sector: Implementation Guidance
- Asset owner/operator perspective
“Cyber threats pose one the gravest national security dangers that the United States faces.”

February 12, 2014  Presidential Statement on the Cybersecurity Framework
“It is the policy of the United States to **enhance the security and resilience** of the Nation’s critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting **safety, security, business confidentiality, privacy, and civil liberties**”
NIST Cybersecurity Framework

• Released February 12, 2014
• Developed in partnership with asset owners and operators, academia, and US Government
• A risk-based cybersecurity approach composed of the following three parts:
  – Core
  – Profile
  – Tiers
• Question: How can a sector address the Framework given the tools they currently use today?
## CORE

Cybersecurity activities, desired outcomes, and common references organized under five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover

### Framework – Components - Core

<table>
<thead>
<tr>
<th>FUNCTION</th>
<th>CATEGORY</th>
<th>SUBCATEGORY</th>
<th>REFERENCES</th>
</tr>
</thead>
</table>
| PROTECT (PR) | | PR.AC-1: Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions. | • CCS CSC 16  
• COBIT 5 DSS05.04, DSS06.03  
• ISA 62443-2-1:2009 4.3.3.5.1  
• ISA 62443-3-2:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9  
• NIST SP 800-53 Rev. 4 AC-2, IA Family |
| PROTECT (PR) | | PR.AC-2: Physical access to assets is managed and protected | • COBIT 5 DSS01.04, DSS05.05  
• ISA 62443-2-1:2009 4.3.3.3.4, 4.3.3.8, 4.3.3.9  
• NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-9 |
| PROTECT (PR) | | PR.AC-3: Remote access is managed | • COBIT 5 APO13.01, DSS01.04, DSS05.03  
• ISA 62443-2-1:2009 4.3.3.6.6  
• ISA 62443-3-3:2013 SR 1.13, SR 2.6  
PROFILE
The alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing “Current” and “Target” Profiles.
TIERS
The degree to which an organization’s cybersecurity risk management practices exhibit the characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive).
The C-Cubed Voluntary Program has 3 goals:

- **First** - Support increasing cyber resilience of critical infrastructure
- **Second** - Increase awareness and use of the NIST Cybersecurity Framework;
- **Third** - Encourage organizations to manage cybersecurity as part of an all hazards approach to enterprise risk management

www.dhs.gov/ccubedvp
Agenda

- Background
- Use of Existing Tools: C2M2 Case Study
- Next Steps for the Energy Sector: Implementation Guidance
- Asset owner/operator perspective
Introduction

Since June 2012, hundreds of organizations have used the C2M2.

DOE has facilitated self-evaluations for utilities servicing an estimated 39 million US consumers.

Business Executives for National Security (BENS) plans to endorse C2M2 for their 400+ members, including Cisco, Amazon, Dell SecureWorks, Lockheed, etc.
C2M2 Program

ES-C2M2
- Public-private collaborative effort
- Sector specific subject matter expertise
- Pilot evaluations

ONG-C2M2
- Tested and refined for ONG through ONG pilot evaluations across upstream, midstream, and downstream ONG companies.

C2M2
- Without sector-specific references or terms of art
- Refined through the ONG pilots, and also via cross-sector outreach

SANS ICS Security Summit
Goals

• Strengthen cybersecurity capabilities

• Enable consistent evaluation and benchmarking of cybersecurity capabilities

• Share knowledge and best practices

• Enable prioritized actions and cybersecurity investments

If requested, DOE facilitates voluntary self-evaluations free of cost. DOE also plans to work with private sector stakeholders to develop energy sector benchmarking based on non-attributable data.
### Industry Use and Adoption

<table>
<thead>
<tr>
<th>Requesting entity type</th>
<th>Organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Utilities</td>
<td></td>
</tr>
<tr>
<td>Cooperative (COOP)</td>
<td>15</td>
</tr>
<tr>
<td>Investor-owned (IOU)</td>
<td>47</td>
</tr>
<tr>
<td>Public power (Muni)</td>
<td>39</td>
</tr>
<tr>
<td>Regional Transmission Organization (RTO)</td>
<td>3</td>
</tr>
<tr>
<td><strong>Total Utilities</strong></td>
<td><strong>104</strong></td>
</tr>
<tr>
<td>Non-utilities</td>
<td>81</td>
</tr>
<tr>
<td>International</td>
<td>22</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>207</strong></td>
</tr>
</tbody>
</table>

DOE also performs facilitated self-evaluations: Roughly 40 completed to date, covering nearly 39 million consumers.
Maturity Model Definition:

- An organized way to convey a path of experience, wisdom, perfection, or acculturation.
- The subject of a maturity model can be an object or things, ways of doing something, characteristics of something, practices, or processes.
## Progression Model Examples

### Progression for Counting

<table>
<thead>
<tr>
<th>Technique</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer</td>
</tr>
<tr>
<td>Calculator</td>
</tr>
<tr>
<td>Adding machine</td>
</tr>
<tr>
<td>Slide rule</td>
</tr>
<tr>
<td>Abacus</td>
</tr>
<tr>
<td>Pencil and paper</td>
</tr>
<tr>
<td>Fingers</td>
</tr>
</tbody>
</table>

### Progression for Authentication

<table>
<thead>
<tr>
<th>Authentication Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Three-factor authentication</td>
</tr>
<tr>
<td>Two-factor authentication</td>
</tr>
<tr>
<td>Passwords change every 60 days</td>
</tr>
<tr>
<td>Strong passwords</td>
</tr>
<tr>
<td>Passwords</td>
</tr>
</tbody>
</table>

### Progression for Human Mobility

<table>
<thead>
<tr>
<th>Movement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fly</td>
</tr>
<tr>
<td>Sprint</td>
</tr>
<tr>
<td>Run</td>
</tr>
<tr>
<td>Jog</td>
</tr>
<tr>
<td>Walk</td>
</tr>
<tr>
<td>Crawl</td>
</tr>
</tbody>
</table>
# Capability Model Examples

## Example 1
- Practices are optimized
- Practices are quantitatively managed
- Practices are defined
- Practices are managed
- Practices are ad hoc

## Example 2
- Practices are externally integrated
- Practices are internally integrated
- Practices are managed
- Practices are performed
- Practices are initiated

## Example 3
- Practices are shared
- Practices are defined
- Practices are measured
- Practices are managed
- Practices are planned
- Practices are performed but ad hoc
- Practices are incomplete
Model Includes 10 Domains

<table>
<thead>
<tr>
<th>Domain</th>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Management</td>
<td>RM</td>
<td>Cybersecurity practices related to risk identification and mitigation.</td>
</tr>
<tr>
<td>Situational Awareness</td>
<td>SA</td>
<td>Practices for understanding and responding to security incidents.</td>
</tr>
<tr>
<td>Workforce Management</td>
<td>WM</td>
<td>Practices for managing personnel and resources related to security.</td>
</tr>
<tr>
<td>Information Sharing and Communications</td>
<td>ISC</td>
<td>Practices for sharing information securely and maintaining data integrity.</td>
</tr>
<tr>
<td>Identity and Access Management</td>
<td>IAM</td>
<td>Practices for managing user access and identity.</td>
</tr>
<tr>
<td>Threat and Vulnerability Management</td>
<td>TVM</td>
<td>Practices for managing threats and vulnerabilities in the system.</td>
</tr>
<tr>
<td>Supply Chain and External Dependencies Management</td>
<td>EDM</td>
<td>Practices for managing dependencies and supply chain risks.</td>
</tr>
</tbody>
</table>

- Domains are logical groupings of cybersecurity practices
- Each domain has an acronym that cross references with the evaluation toolkit
The Model at a Glance

<table>
<thead>
<tr>
<th>Maturity Indicator Levels</th>
<th>3 Managed</th>
<th>2 Performed</th>
<th>1 Initiated</th>
<th>0 Not Performed</th>
</tr>
</thead>
</table>

**4 Maturity Indicator Levels:** Defined progressions of practices

Each cell contains the defining practices for the domain at that maturity indicator level

**10 Model Domains:** Logical groupings of cybersecurity practices

- Risk Management
- Asset Change and Configuration Management
- Identity and Access Management
- Threat and Vulnerability Management
- Situational Awareness
- Information Sharing and Communications
- Event and Incident Response, Continuity of Operations
- Supply Chain and External Dependencies Management
- Workforce Management
- Cybersecurity Program Management

SANS ICS Security Summit
Organization of a Domain

Model contains 10 domains

Approach Objectives

- Practices at MIL1
- Practices at MIL2
- Practices at MIL3

(one or more per domain)
Unique to each domain

Management Objectives

- Practices at MIL2
- Practices at MIL3

(one or more per domain)
Similar in each domain

Approach objectives are supported by a progression of practices that are unique to the domain.

Each management objective is supported by a progression of practices that are similar in each domain and describe institutionalization activities.
## Maturity Indicator Levels

<table>
<thead>
<tr>
<th>Level</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIL0</td>
<td>Not Performed</td>
<td>• MIL1 has not been achieved in the domain</td>
</tr>
<tr>
<td>MIL1</td>
<td>Initiated</td>
<td>• Initial practices are performed, but may be ad hoc</td>
</tr>
</tbody>
</table>
| MIL2  | Performed             | • Practices are documented  
• Stakeholders are involved  
• Adequate resources are provided for the practices  
• Standards or guidelines are used to guide practice implementation  
• Practices are more complete or advanced than at MIL1 |
| MIL3  | Managed               | • Domain activities are guided by policy (or other directives)  
• Activities are periodically reviewed for conformance to policy  
• Responsibility and authority for practices are clearly assigned to personnel with adequate skills and knowledge  
• Practices are more complete or advanced than at MIL2 |
There are 2 practices at MIL1 for the Risk Domain.

Outer ring and number(s) summarize implementation state of those practices; in this case, both practices are fully implemented.
To achieve MIL2, requires 13 practices in total, including the 2 from MIL1.

11 practices are fully implemented.

2 practices are not implemented.
Scoring

Sample Summary Score

SANS ICS Security Summit
Report

Sample Summary Score

[Sans Ics Security Summit]
Agenda

Background

Use of Existing Tools: C2M2 Case Study

Next Steps for the Energy Sector: Implementation Guidance

Asset owner/operator perspective
C2M2 and Framework Implementation Guidance

MILs, Tiers, Profiles, and Scorecards... Confused yet?

• Several sectors are working on Framework Guidance to remove the confusion and speak plainly regarding the use of existing tools and programs

• C2M2, like many other existing tools that are well-vetted with industry, act as Framework enablers for implementation.
  – Some tools are better equipped to address the Framework than others… how many standards have the concept of progressing a program or capability?
  – C2M2 is a self-assessment methodology

• Like the Framework itself, any sector guidance will also be voluntary.
Executive Order 13636
Improving Critical Infrastructure Cybersecurity
Section 8(b)

“Sector-Specific Agencies, in consultation with the Secretary and other interested agencies, shall coordinate with the Sector Coordinating Councils to review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments.”

- DOE is working with sector to develop an implementation guidance document.
- The guidance document will address the C2M2 and other industry approaches for framework implementation.
Stakeholder Engagement

DEPARTMENT OF ENERGY
Framework Implementation Guidance Development

GUIDELINE DEVELOPMENT
Electricity Subsector Coordinating Council (ESCC) / Senior Executive Work Group (SEWG) / Framework Implementation Sub-Team

GUIDELINE DEVELOPMENT
Oil & Natural Gas Subsector Coordinating Council (ONG SCC) / Cybersecurity Work Group / Framework Implementation Team

SECTOR ENGAGEMENT EVENTS

CROSS SECTOR COLLABORATION
Transportation - TSA, Coast Guard

PUBLIC SECTOR COLLABORATION
Energy Government Coordinating Council (GCC)
DHS C³ Voluntary Program
White House
NIST

SANS ICS Security Summit
Electricity Subsector - Progress

- DOE and the Electricity Subsector Coordinating Council (ESCC) / Senior Executives Work Group (SEWG) / Framework Guidance Sub-Team held a kick-off meeting on February 13th, 2014

- The team is currently reviewing guidance development approach, C2M2-Framework mapping and a proposed outline for the Framework Implementation Guideline document.

- The team will meet on bi-weekly basis to support guidance development efforts. The resulting document will be used to publish a notice in the Federal Register to seek formal sector comments.
C2M2 and Framework Implementation Guidance

• There are many potential tools for addressing Framework implementation. The C2M2 is one of many such tools.

• For organizations that use C2M2, the Implementation Guidance will highlight the interoperability between the NIST Cybersecurity Framework and DOE’s C2M2 program. For example:
  – **C2M2 Practices**, which cover elements of both the Framework Core and Tier characterizations, address both sophistication of a cybersecurity program, as well as the culture, or institutionalization supporting it.
  – **C2M2 Maturity Indicator Levels (MILs)**, a measure of the progression within a C2M2 domain as a cybersecurity program develops, tie with elements of the Framework Tiers. Each of the domain MIL scores in the C2M2 incorporate elements of the risk management characteristics from the Tiers.
  – **C2M2 Scorecards**, which highlight the level of maturity across C2M2 domains, are almost identical to the concept of Framework Profiles, both current and target.

• For organizations that prefer an implementation approach other than the C2M2, DOE will work with the SCCs to develop and incorporate the alternative approaches in the guidance document to satisfy the framework requirements.
Agenda

- Background
- Use of Existing Tools: C2M2 Case Study
- Next Steps for the Energy Sector: Implementation Guidance
- Asset owner/operator perspective
Duke Energy adopted the ES-C2M2 model to baseline current practices and to establish desired maturity levels across the ten domains.

This project involved legacy teams from Transmission, Generation, NERC Corporate Compliance, IT, and Enterprise Protective Services (physical) and included the following activities:

- Educated & trained project team members on the Cybersecurity Capability Maturity Model (ES-C2M2)
- Mapped NERC CIP Reliability Standards and Requirements to the domains in the model
- Assessed current maturity level of the organization (facilitated by the Department of Energy)
- Developed action items, prioritization & implementation plans

Creating a new business case for ES-C2M2 adoption throughout the company
Asset owner/operator perspective

• Scope
  – Critical infrastructure is defined in the EO as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”

• What does adoption mean?
  – Adoption = DHS language “any organization that uses the Framework as a part of its process to identify and manage cyber risk has “adopted” the Framework”
  – "provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach," implementation of the Framework should focus on the systems and assets essential to critical infrastructure functions.
  – What is essential to critical infrastructure function will vary by organization.
Asset owner/operator perspective

• Multiple sector alignment
  – Commercial Facilities, Chemical
  – Communications
  – Dams
  – Energy (electric and oil and natural gas sub-sectors)
  – Nuclear Reactors, Materials, and Waste
  – Transportation Systems
  – Water and Wastewater Systems
  – Chemical
Some of the top tools used in the energy sector:

- ES-C2M2
- ES-RMP
- NERC CIPv5
- TSA Pipeline Security Guideline
- NIST 800-53
- NIST 7628
- Chemical Facility Anti-Terrorism Standards
- Maritime Transportation Security Act
Asset owner/operator perspective – Implementation

• EO 13636 Sec. 8 (b):

“Sector-Specific Agencies, in consultation with the Secretary and other interested agencies, shall coordinate with the Sector Coordinating Councils to review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments”

• Sector-Specific Agency = DOE is primary

• Sector Coordinating Council = Electricity Sub-Sector Coordinating Council (ESCC)
Electricity Subsector Coordinating Council (ESCC)

Leadership (3): 1 chair, 2 vice chairs

Steering Committee (9): NIAC representative, APPA, CEA, EEI, EPSA, ISO/RTO Council, NEI, NERC, NRECA

Asset Owners (18): CEOs proportionally representing asset owners from across industry segments

Electricity Subsector Information Sharing and Analysis Center (ES-ISAC)
Day-to-day operations run by NERC

Electricity Subsector Coordinating Council (ESCC)

30 member body to serve as the principle entity coordinating with government counterparts on planning, preparedness, resilience, and recovery issues related to national security issues affecting the electric grid.
ESCC – working groups and sub teams

- Mechanism for industry-government coordination to prepare for and respond to national-level threats to critical infrastructure
- ESCC is CEO level
- Senior Executive Working Group (SEWG) – senior executives, e.g., COOs, CIOs, CISOs
- SEWG Sub Teams
  - Flow of Information
  - Playbook Development & Incident Response
  - Cyber Framework Implementation
ESCC – SEWG Cyber Framework
Implementation Sub Team

• Began the discussion
  • Kick off February 28th
    • Implementation guidance planned to be complete in 90 days
• Industry – need for mapping existing cybersecurity guides to the Framework to identify overlap and gaps
• Government – prefers high-level implementation guide, which lists the key cybersecurity “tools” used by the sector
• Perhaps we can do both?
  • Keep the implementation guidance high-level
  • Develop more detailed maps within industry
THANK YOU

For questions or feedback please contact

JASON.CHRISTOPHER@HQ.DOE.GOV

EDWIN.GOIFF@DUKE-ENERGY.COM

SAMARA_N_MOORE@NSC.EOP.GOV

Nadya.bartol@utc.org
RESOURCES


C3 Voluntary Program: www.dhs.gov/ccubedvp

C2M2 Program: http://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program