U.S. DEPARTMENT OF
ENERGY

Office of Electricity Delivery and Energy Reliability

Use of the NIST Cybersecurity Framework & DOE C2M2

Overview

Recognizing that the national and economic security of the United States depends on the reliable functioning of critical infrastructure, the President under the Executive Order (EO) 13636 "*Improving Critical Infrastructure Cybersecurity*" of February 2013 directed National Institute of Standards and Technology (NIST) to work with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructure.

Through an open and collaborative process, NIST engaged individuals, organizations, academia, and owners and operators of critical infrastructure to develop a flexible, repeatable, and cost-effective approach for the framework. On February 12, 2014 NIST will release its Cybersecurity Framework for use across all critical infrastructure sectors.

Executive Order 13636

- Develop a technology-neutral voluntary cybersecurity framework
- Promote and incentivize the adoption of cybersecurity practices
- Increase the volume, timeliness and quality of cyber threat information sharing
- Incorporate strong privacy and civil liberties protections into every initiative to secure our critical infrastructure
- Explore the use of existing regulation to promote cyber security

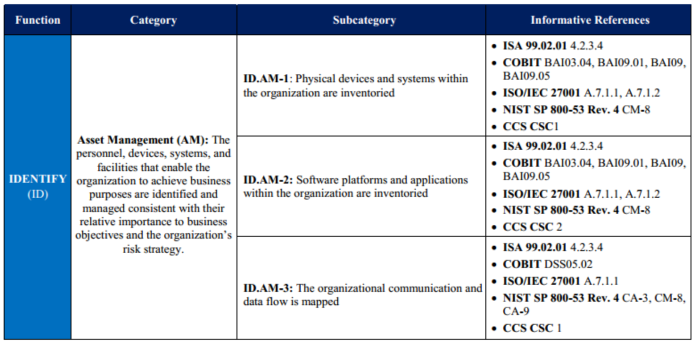
Moving forward, the Department of Energy (DOE) will engage the Sector Coordinating Councils (SCC), owners and operators of energy delivery systems, and subject matter experts across the energy sector to develop implementation guidance for the Framework based on the sector's experience with DOE's Cybersecurity Capability Maturity Model (C2M2) and other existing practices.

NIST Cybersecurity Framework Components

The NIST framework is a risk-based cybersecurity approach composed of the following three parts:

FRAMEWORK CORE

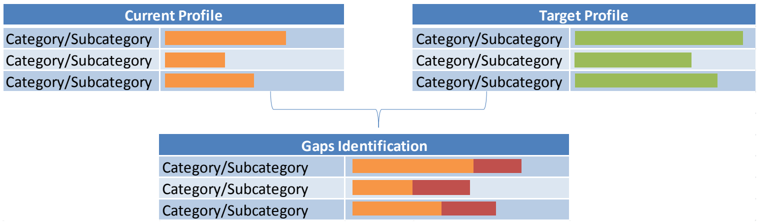
- Set of cybersecurity activities and references that are common across critical infrastructure sectors organized around particular outcomes
- Consists of five Functions (*Identify, Protect, Detect, Respond, and Recover*) that provide a strategic view of an organization's cybersecurity risk management
- Identifies key Categories and Subcategories underlying each of these Functions, and matches them with example Informative References (standards, guidelines, and practices)



Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (AM):** The personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	• **ISA 99.02.01** 4.2.3.4 • **COBIT** BAI03.04, BAI09.01, BAI09, BAI09.05 • **ISO/IEC 27001** A.7.1.1, A.7.1.2 • **NIST SP 800-53 Rev. 4** CM-8 • **CCS CSC**1
		ID.AM-2: Software platforms and applications within the organization are inventoried	• **ISA 99.02.01** 4.2.3.4 • **COBIT** BAI03.04, BAI09.01, BAI09, BAI09.05 • **ISO/IEC 27001** A.7.1.1, A.7.1.2 • **NIST SP 800-53 Rev. 4** CM-8 • **CCS CSC** 2
		ID.AM-3: The organizational communication and data flow is mapped	• **ISA 99.02.01** 4.2.3.4 • **COBIT** DSS05.02 • **ISO/IEC 27001** A.7.1.1 • **NIST SP 800-53 Rev. 4** CA-3, CM-8, CA-9 • **CCS CSC** 1

FRAMEWORK PROFILE

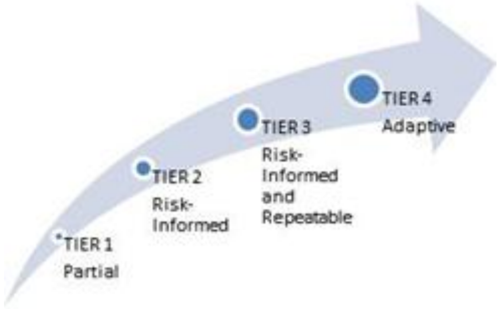
- Represents the outcomes that a particular system or organization has achieved or is expected to achieve as specified in the Framework Categories and Subcategories
- Can be used to identify and prioritize opportunities for improvement by comparing a "Current" Profile with a "Target" Profile



Use of the NIST Framework & DOE C2M2

FRAMEWORK IMPLEMENTATION TIERS

- Tiers describe the degree to which an organization's cybersecurity risk management practices exhibit characteristics such as risk and threat aware, repeatable, and adaptive
- Tiers characterize an organization's practices over a range, from Partial (Tier 1) to Adaptive (Tier 4), progressing from informal, reactive implementations to approaches that are agile and risk-informed



Use of the Energy Department's C2M2 with the Framework

The C2M2 is one of many potential tools for addressing Framework implementation. (Versions of the C2M2 are available for the electricity and oil and natural gas subsectors, and for other industries.) Since the beginning of the C2M2 program in June 2012, hundreds of organizations have used the C2M2. DOE has facilitated self-assessments for utilities servicing an estimated 39 million consumers in the United States. For energy sector organizations that use the C2M2 as a measurement and investment decision tool, the DOE, in partnership with NIST and the Department of Homeland Security (DHS), is working on guidance documents that will highlight the interoperability between the NIST Cybersecurity Framework and DOE's C2M2 program. The Framework and C2M2 share many core elements. 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.

The Department has engaged the electricity, and oil & natural gas SCCs and is working with asset owners and operators, as well as security specialists, to address the many ways the energy sector may choose to implement the Framework. A final mapping of the Framework will be incorporated into a public-private partnership guidance document to be made public in mid-2014.

Additional information on the NIST Preliminary Cybersecurity Framework may be obtained by contacting cyberframework@nist.gov.

Additional information on DOE's Cybersecurity Capability Maturity Model (C2M2) may be obtained by contacting C2M2@doe.gov.