Building the NIST AI RMF Workshop

Exactly What Is An AI RMF Profile?

Cherilyn Pascoe | Senior Tech Policy Advisor & Lead, NIST CSF Program

October 18, 2022

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST AI RMF Profiles

Use-case profiles

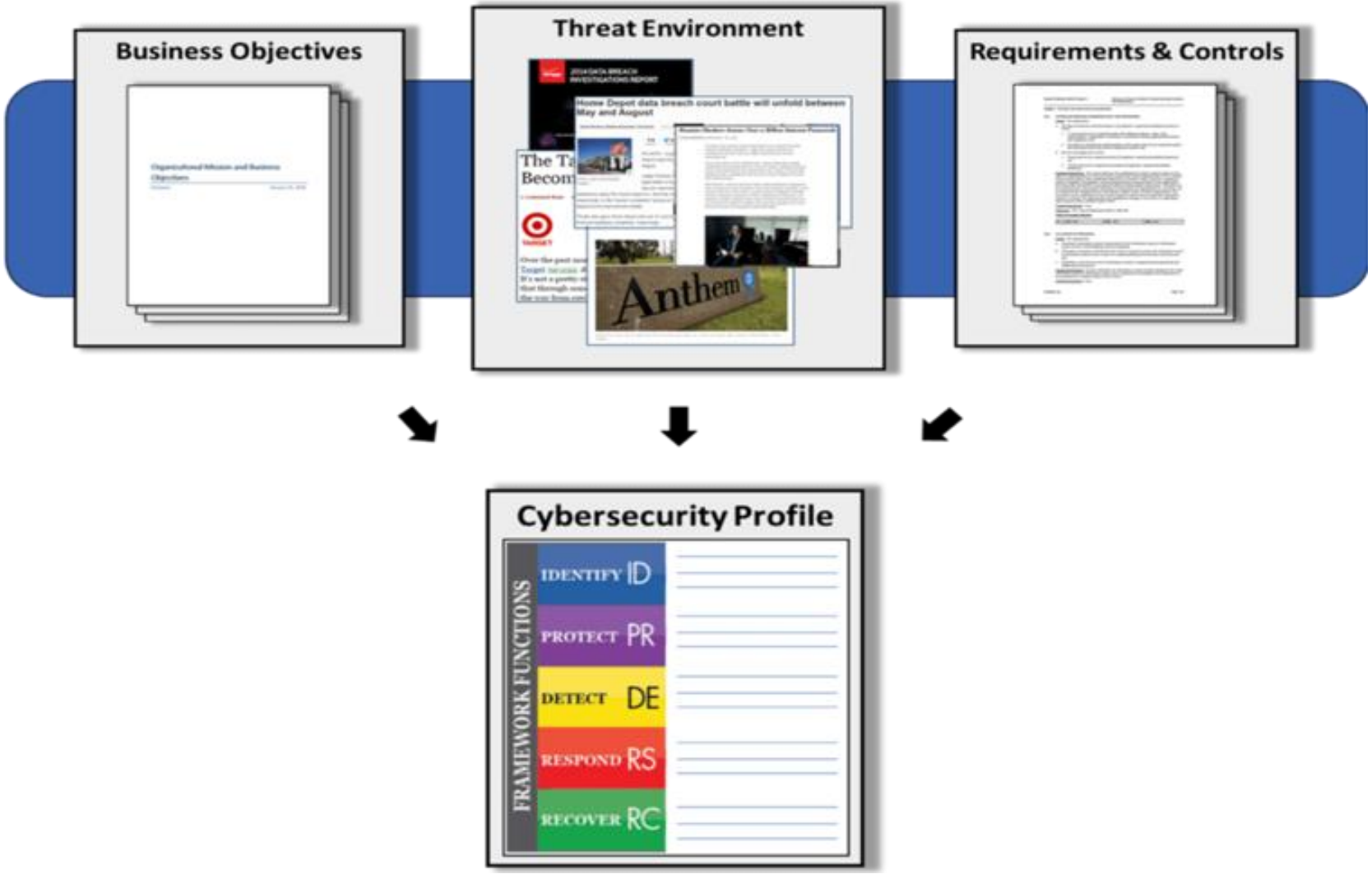
- Instantiations of the AI RMF functions, categories, and subcategories for a certain application or use case based on the requirements, risk tolerance, and resources of the Framework user

Temporal profiles

- Descriptions of either the current state or the desired, target state of specific AI risk management activities within a given sector, industry, organization, or application context

NIST welcomes contributions towards development of AI RMF profiles

NIST Cybersecurity Framework Profiles



NIST Cybersecurity Framework Profiles

NIST CSF Sample Profiles - https://www.nist.gov/cyberframework/examples-framework-profiles

- NISTIR 8183 - Cybersecurity Framework Manufacturing Profile
- NISTIR 8374 - Ransomware Risk Management: A Cybersecurity Framework Profile
- NISTIR 8183r1 - Cybersecurity Framework Version 1.1 Manufacturing Profile
- NISTIR 8310 (Draft) - Cybersecurity Framework Election Infrastructure Profile
- NISTIR 8323 - Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services
  - **Draft** NISTIR 8323 Revision 1 | Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services
- NIST TN 2051 - Cybersecurity Framework Smart Grid Profile
- **Draft** White Paper NIST CSWP 27 | Cybersecurity Profile for Hybrid Satellite Networks (HSN) Draft Annotated Outline
- Maritime Bulk Liquids Transfer Cybersecurity Framework Profile - US Coast Guard
- Cybersecurity Framework Botnet Threat Mitigation Profile - Cybersecurity Coalition
- Cybersecurity Framework DDoS Threat Mitigation Profile - Cybersecurity Coalition
- The Profile - Cyber Risk Institute
- Framework Payroll Profile - IRS Security Summit
- Cybersecurity Framework Profile: White House Fact Sheet - Seemless Transition

NIST Cybersecurity Framework Profiles

NIST Cybersecurity Framework Profile for Positioning, Navigation, and Timing (PNT) (NISTIR 8323): https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8323.pdf

Table 3 - Identify – Asset Management Subcategories Applicable to PNT

Identify Asset Management Subcategory	Applicability to PNT	References (PNT-Specific)
AM-1: **Physical devices and systems within the organization are inventoried.**	Document and maintain an inventory of the PNT system components that reflect the current system. The physical inventory should include PNT system components used to support critical infrastructure/operations and critical system components that rely on PNT data and services to properly function. PNT system components may include GNSS receivers, wireless local area network (WLAN) receivers, terrestrial beacon system receivers (TBS), radio navigation or timing antennas, network switches, Internet of Things (IoT)/ Supervisory Control and Data Acquisition (SCADA) devices, NTP and Precision Time Protocol (PTP) servers, positioning sensors, clocks, etc. Cryptographic modules, test and measurement equipment, navigation systems, etc. are examples of hardware and devices dependent on PNT services. Incorporate a configuration management tool that documents locations of all PNT antennas and verify with physical inspections. During physical inspections, identify equipment associated with PNT devices and locate PNT service provider interfaces, such as GNSS antennas.	**3GPP TS 36.305** 4.3 **DHS CISA** 1.a, 2.a **ICAO 9849** 1.4 **IEEE 1588** 6, 9, 10 **IEEE 802.1AS** 7, 11 **IEEE 2030.101** 4.6, 4.7, 4.8, 4.9 **NIST SP 800-53 Rev. 5** CM-8, CM-9 PM-5 **NIST SP 800-160 Rev. 1** 2.3 **RTCA 229** 2.1.5.2.1, 2.4, 2.5 **RTCA 292** 2.5 **RTCA 326** 3.1 **USG FRP** 1.7.8, 4.4.2, 4.6, 5.1.2, 6

NIST Cybersecurity Framework Profiles

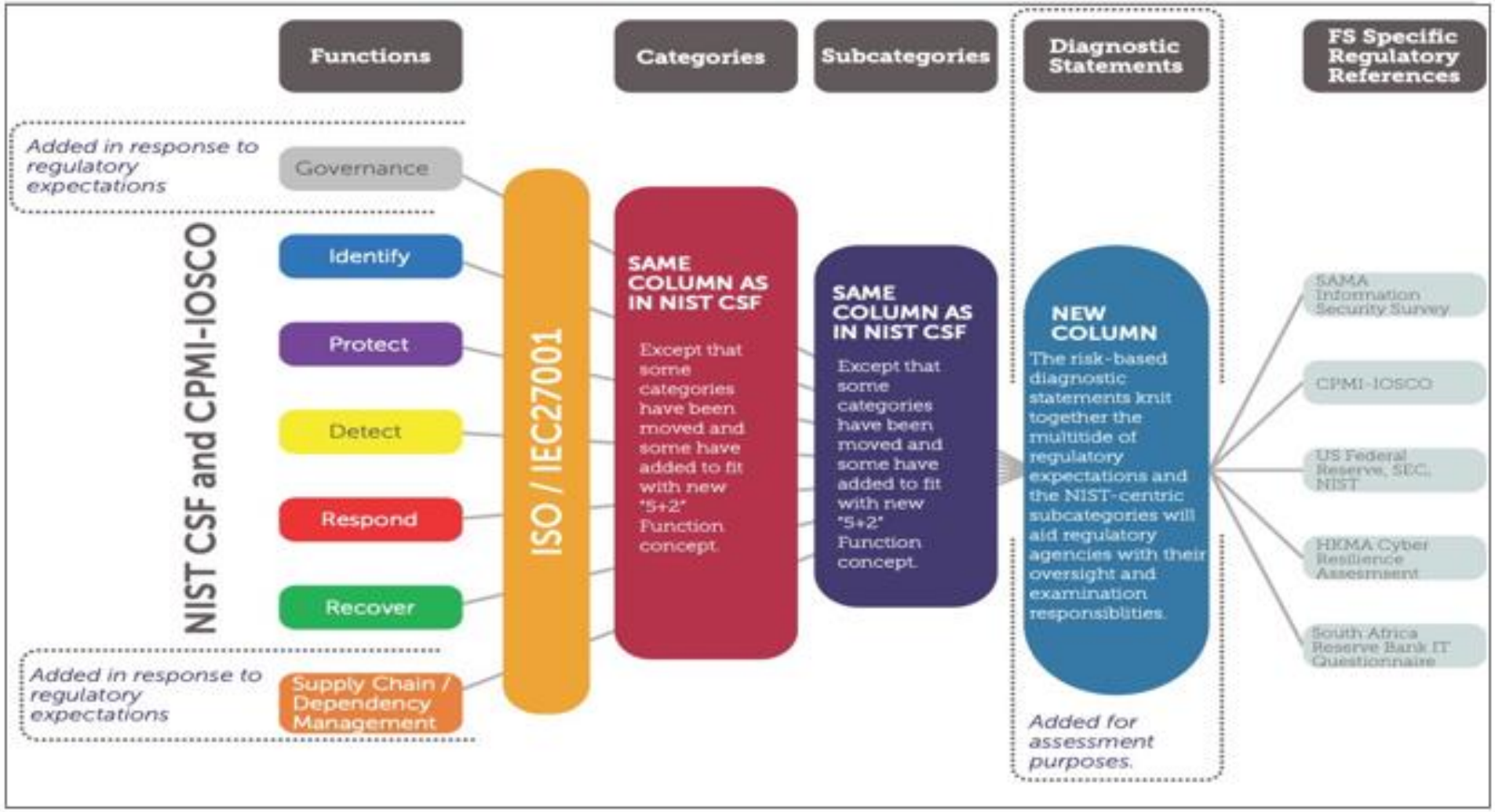
NIST Cybersecurity Framework Profile for the Smart Grid (TN 2051): https://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.2051.pdf

Table 3 - IDENTIFY Subcategories Prioritization and Considerations

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power System Owners/Operators
Category		Subcategories				
ID	Asset Management	ID.AM-1	ID.AM-1	ID.AM-1	ID.AM-1	Knowing hardware assets is critical for maintaining safety, reliability, and resilience, as well as facilitating the transition to the modern grid. Legacy and modernized assets[10] need to be known and understood. As modernized grids become more distributed, power system owners/operators need to be accountable for all distributed assets that they own.
		ID.AM-2	ID.AM-2	ID.AM-2	ID.AM-2	Knowing software assets is critical for maintaining reliability, and resilience, as well as facilitating the transition to the modern grid. Legacy and modernized assets need to be known and understood. This especially applies to modernized assets because the sophisticated logic that they execute is driven by software.
		ID.AM-3	ID.AM-3	ID.AM-3	ID.AM-3	Understanding communication and data flows is important to ensure reliability and resilience. Communications networks are critical for modernized grids, and understanding the different types of data flows (control, monitoring, and management) will provide critical information for managing those flows within modernized infrastructures and between modernized and traditional infrastructure.

NIST Cybersecurity Framework Profiles

CRI Cybersecurity Framework Profile for Financial Sector:
https://cyberriskinstitute.org/the-profile/



NIST AI RMF Profiles

Panel: What Exactly Is an AI RMF Profile?

Use-case profiles

- Instantiations of the AI RMF functions, categories, and subcategories for a certain application or use case based on the requirements, risk tolerance, and resources of the Framework user

Temporal profiles

- Descriptions of either the current state or the desired, target state of specific AI risk management activities within a given sector, industry, organization, or application context

NIST welcomes contributions towards development of AI RMF profiles