Benefits of Updated Mapping between the NIST Cybersecurity Framework and the NERC Critical Infrastructure Protection Standards

August 2021

Every organization in the electricity sector knows that cybersecurity is already a major challenge. There are a variety of standards and resources that organizations are either required or encouraged to use in managing their unique cybersecurity-related risks. A recent mapping initiative between two major cybersecurity guidance documents can help organizations mature and align their compliance and security programs and better manage risks.

Function	Category Unique Identifier	Category
Identify	ID. AM	Asset Management
	ID. BE	Business Environment
	ID. GV	Governance
	ID.RA	Risk Assessment
	ID.RM	Risk Management Strategy
	ID.SC	Supply Chain Risk Management
Protect	PR.AC	Identity Management and Access Control
	PR.AT	Awareness and Training
	PR.DS	Data Security
	PR.IP	Information Protection and Procedures
	PR.MA	Maintenance
	PR.PT	Protective Technology
Detect	DE.AE	Anomalies and Events
	DE.CM	Security Continuous Monitoring
	DE.DP	Detection Processes
Respond	RS.RP	Response Planning
	RS.CO	Communications
	RS.AN	Analysis
	RS.MI	Mitigation
	RS.IM	Improvements
Recover	RC.RP	Recovery Planning
	RC.IM	Improvements
	RC.CO	Communications

Figure 1 - CSF Functions and Categories

NERC's Critical Infrastructure Protection (CIP) Reliability Standards are a set of requirements designed to mitigate the risk of a compromise that could lead to misoperation or instability in the Bulk Electric System (BES). The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES. The Reliability Standards cover topics like the identification and protection of BES Cyber Assets, defining logical isolation perimeters, personnel and training, BES Cyber System security management, disaster recovery planning, physical security, and supply chain risk management.

The Framework for Improving Critical Infrastructure Cybersecurity – commonly referred to as the Cybersecurity Framework (CSF)[1] – is a risk-

[1] https://www.nist.gov/cyberframework

based approach to help owners and operators of critical infrastructure manage cybersecurity-related risk in a manner complementary to an organization's existing cybersecurity and risk management processes. The CSF was developed by the National Institute of Standards and Technology (NIST) in close collaboration with the private sector. It is used by organizations of all sizes, in a variety of sectors, and globally. The Framework Core (Core) uses common language to provide a catalog of desired cybersecurity activities and outcomes. Using five concurrent and continuous Functions as an organizing structure—Identify, Protect, Detect, Respond, and Recover—the Core provides a high-level, strategic view of an organization's management lifecycle for cybersecurity risk. Underlying the five concurrent Functions, the Core identifies 23 Categories (as shown in **Figure 1**) and 108 Subcategories that describe discrete cybersecurity outcomes. The Core also presents informative references for each of the Subcategories that include industry standards, guidelines, and practices.

These informative references provide practical suggestions for how organizations can achieve the desired outcome of each Subcategory. An example of two Subcategories within the Supply Chain Risk Management Category is shown in **Figure 2**. A dynamic set of informative references is available through the NIST Online Informative References Program (OLIR[2]).

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess, and manage supply chain risks.	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	• **CIS CSC** 4 • **COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 • **ISA 62443-2-1:2009** 4.3.4.2 • **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 • **NIST SP 800-53 Rev. 4** SA-9, SA-12, PM-9
		ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	• **COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 • **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 • **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 • **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-12, SA-14, SA-15, PM-9

Figure 2 - Two Subcategories and Relevant Informative References

These two approaches to cybersecurity—NERC's Standards-driven cybersecurity requirements and NIST's framework for assessing and mitigating cybersecurity risk—are complementary. A recent International Energy Agency report[3] on cyber resilience in electricity systems emphasizes the need to combine requirements-driven regulatory approaches with framework-based management strategies to ensure

[2] https://csrc.nist.gov/projects/olir

[3] IEA (2021). Enhancing Cyber Resilience in Electricity Systems. Paris, France: https://webstore.iea.org/download/direct/4359

power grid cybersecurity. NERC and NIST personnel have partnered to update the mapping between NERC CIP and the CSF to provide confidence to organizations seeking to secure their electric system infrastructure and operations.

An initial mapping between the CSF V1.0 and NERC CIP Standards (both Versions 3 and 5) was completed in late 2014 by the NERC Control Systems Security Working Group, which was part of the former NERC Critical Infrastructure Protection Committee. Since that time, both the NERC CIP Standards and the CSF have been updated, and a new mapping was needed. Building on the 2014 effort, NERC and NIST updated the mapping to reflect the CSF V1.1 and latest NERC CIP Reliability Standards. In the spring of 2020, the NERC Compliance Input Working Group—now known as the Security Working Group (SWG) that is a part of the Reliability and Security Technical Committee—reviewed the mapping and provided recommendations for improving the resource.

The final mapping[4] includes three distinctive spreadsheet tabs, described as follows:

- **NIST CSF 1.1 to CIP v5** is oriented toward the CSF Subcategories. This tab shows the NERC CIP Standards that map to each Subcategory of the CSF Core. A row is included for each unique mapping between a NERC CIP Standard and a CSF Subcategory. For that reason, a Subcategory may appear in consecutive rows. For example, the Subcategory ID.AM-1 has two rows because two NERC CIP Standards map to that Subcategory. Each row also includes a justification for the mapping, provides mappings to relevant Cybersecurity Capability Maturity Model (C2M2)[5] practices, and lists industry recommended implementation guidance.
- **CIPv5 to CSF 1.1 XREF** reverses the mapping (i.e., focusing on NERC CIP Standards) and lists the CSF Subcategories that align with each NERC CIP Standard requirement. A NERC CIP Standard (e.g., CIP-002-5.1a-R1) may span multiple rows if it contains multiple requirements (e.g., CIP-002-5.1a-R1-1.1).
- **Pivot** shows the same information as the "CIPv5 to CSF 1.1 XREF" tab but is configurable. Users can expand or minimize each NERC CIP Standard. They can also choose additional information to view, including Function, Category, and Subcategory information from the Cybersecurity Framework; C2M2 maturity indicator levels for each Subcategory; or guidance from the first tab.

Compliance and Security

The mapping spreadsheets show which Subcategories—and the informative references by extension—can help organizations achieve a more mature CIP requirement compliance program. Along with the compliance maturity, the user gains additional resources on how to improve their security posture and potentially reduce their organization's security and business risks. The OLIR program can help users find additional informative references for each CIP Requirement, making the compliance programs more efficient and effective.

[4] https://www.nerc.com/pa/comp/CAOneStopShop/NIST%20CSF%20v1.1%20to%20NERC%20CIP%20FINAL.XLSX
https://doi.org/10.18434/mds2-2348
[5] https://www.energy.gov/ceser/energy-security/cybersecurity-capability-maturity-model-c2m2-program

To gain a quick understanding of a Subcategory and how it could apply to the CIP program, a user can look at the Guidance column in the "NIST CSF 1.1 to CIP v5" tab. Industry subject matter experts developed this guidance; however, this guidance is limited to a generic, low level of detail.

In contrast to the high-level guidance, an organization can utilize the mapping, along with the informative references, to develop an in-depth program to reduce risks across the board. The wealth of information in the Core's informative references is immense; this mapping offers a good first step for users unsure of where to start. For example, if the goal is to implement a more mature baseline program, the pivot table can be used to look for CIP-010-2 Requirement R1; eight Subcategories that map to that CIP Requirement are shown. Consider two of these Subcategories, Protect (PR) Data Security (DS) Subcategories 6 and 7. PR.DS-6 states, "*Integrity checking mechanisms are used to verify software, firmware, and information integrity,"* and PR.DS-7 states, "*the development and testing environment(s) are separate from the production environment*." These outcomes sound desirable, but it is not immediately clear from this description how an organization could achieve that goal. The Core's list of informative references can help users understand the steps their organization can take to realize the outcomes. For PR.DS-6, the Core lists these informative references:

- **Center for Internet Security (CIS) Critical Security Controls (CSC)** 2 and 3
- **Control Objectives for Information and Related Technologies (COBIT) 5** API01.06, BAI06-01, and DSS06-02
- **International Society of Automation (ISA) 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, and SR 3.8
- **International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001:2013** A.12.2.1, A.12,5,1; A.14.1.2, A.14.1.3, and A.14.2.4
- **NIST Special Publication (SP) 800-53 Rev 4** SC-16 and SI-17

With these informative references, an organization will be able to develop an action plan. An organization could add even more depth by looking at NIST's OLIR program for additional informative references. The mapping is intended to help an organization mature its compliance and security programs, as they should be aligned. Subject matter experts are developing a companion tool to facilitate industry use of the NERC CIP-to-CSF mapping. The tool uses the mapping to help organizations self-assess their current security and compliance posture and develop an improvement plan for addressing identified gaps. The tool is the result of a collaborative effort by industry volunteers from NERC's Reliability and Security Technical Committee Security Working Group and representatives from NERC and NIST.