NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NIST CSF to NERC CIP Standards Mapping

Navigating the Mapping on the NIST National Online Informative Reference (OLIR) Program

2023

RELIABILITY | RESILIENCE | SECURITY




Purpose

- The National Online Informative References (OLIRs) Program is a National Institute of Standards and Technology (NIST) effort to facilitate subject matter experts in defining standardized online informative references between elements of their documents (Reference Document) and elements of NIST documents (Focal Document).
- NIST and the North American Electric Reliability Corporation (NERC), in a joint effort, mapped the elements between the Cybersecurity Framework Core (CSF) v1.1 and The Critical Infrastructure Protection (CIP) Cyber Security Reliability Standards to provide a better understanding of the measures to enhance the security of the national grid.

Objectives

- Able to Describe The CSF Core and CIP Reliability Standard
- Understand the Mapping
  - Informative Reference
  - Focal and Reference Documents
  - Focal Elements Map to Reference Elements
  - Rationale Options
  - Relationship Options
  - Strength of Relationship Options
  - Informative Reference Mapping
- How to Update the Mapping
- Project Team and Contact Info
- OLIR Demo

CSF Core and CIP Descriptions

- CSF Core Consists of Three Elements:
  - Functions – organize basic cybersecurity activities at their highest level, helping organizations express management of cybersecurity risk
  - Categories – subdivisions of a function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities
  - Subcategories – divide a category into specific outcomes of technical and/or management activities
- CIP Consists of a Family of Reliability Standards:
  - Mandatory for the electricity segment of the energy sector
  - 12 cyber security and 1 physical security Reliability Standard work collectively
  - Covers asset identification, management controls, personnel security, network and system security, physical security, incident response, supply chain, information security, change management, and data communications

Understand The Mapping

- An *Informative Reference* is a relationship between an element of one document relating to an element of another document.
- Focal Document – NIST document as the basis for comparison; Framework for Improving Critical Infrastructure Cybersecurity v1.1 (April 16, 2018)
- Reference Document – a document being compared to a Focal Document; Reliability Standards for the Bulk Electric System (BES) of North America (December 6, 2022), specifically the CIP Section
- Mapped Each CIP Reliability Standard requirement to the CSF Function, Category, and Subcategory
  - Categorized the mapped elements:
    - Rationale, Relationship, and Strength of Relationship

Understand The Mapping: Rationale

- Rationale options for each Informative Reference:
  - Syntactic—the two elements use the same words or have identical syntax
    - printf (“bar”); [… C programming language]
    - printf (“bar”); [… C programming language]
  - Semantic—the two elements have the same meaning; the same thing
    - “The organization employs a firewall at the network perimeter.”
    - “The enterprise uses a device that has a network protection application installed to safeguard the network from intentional or unintentional intrusion.”
  - Functional—the two elements achieve the same result or outcome
    - printf (“foo\n”); [… C programming language]
    - print “foo” [… BASIC programming language]

Understand The Mapping: Relationship

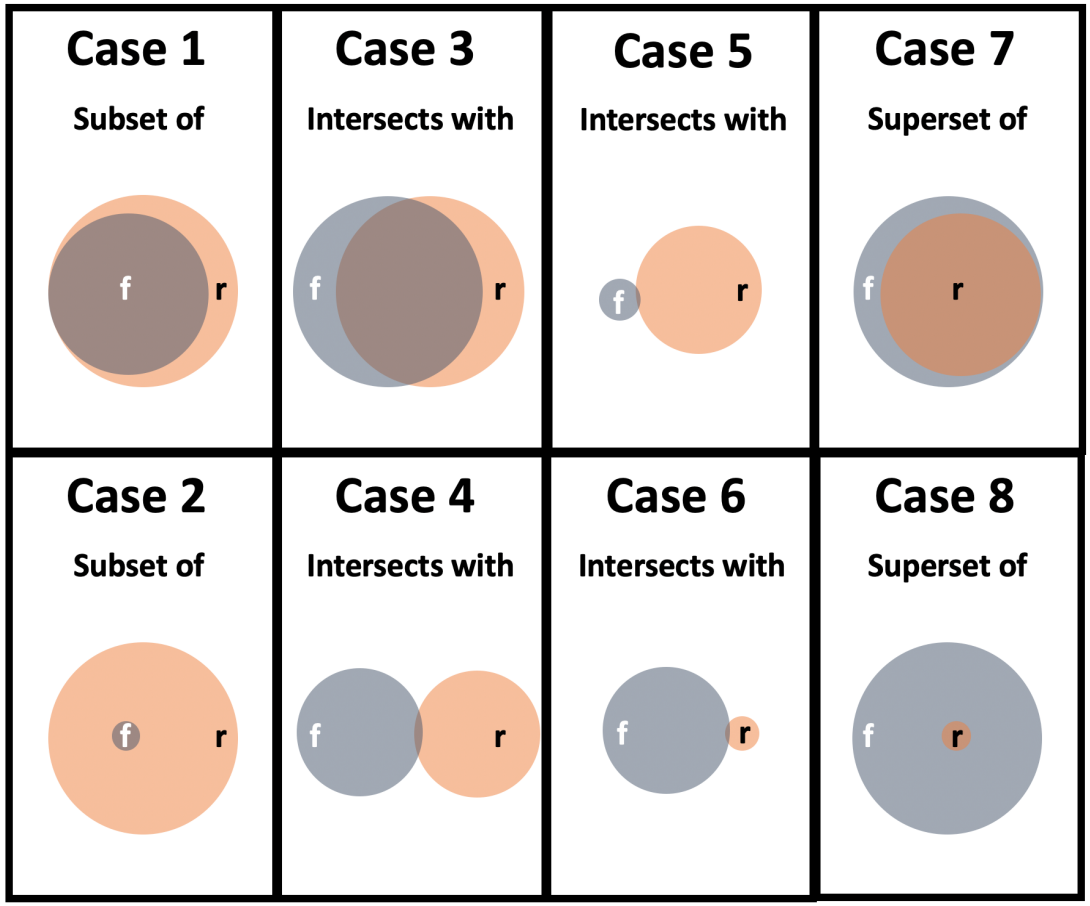
- Relationship options for each Informative Reference:
  - Subset of—the wording in NIST CSF element is a subset of the wording in NERC CIP element. That is, the NERC CIP Reliability Standard language covers everything that is in the CSF Subcategory and has even more
  - Intersects with—the CSF Subcategory language and the NERC CIP Reliability Standard language have some concepts in common, but they each have unique concepts not covered by the other
  - Superset of—the wording in NIST CSF element is a superset of the wording NERC CIP element. That is, the CSF Subcategory language covers everything that is in the NERC CIP Reliability Standard and has even more
  - Equal to—the concepts in both the CSF Subcategory and the NERC CIP Reliability Standard have all the same concepts and nothing different
  - Not related to—NIST CSF element and NERC CIP element do not have anything in common

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Understand The Mapping: Strength of Relationship

- Strength of Relationship (SOR) for an Informative Reference element is intended for lateral comparisons, like the CSF and the CIP Reliability Standards, and not comparisons of documents at vastly different levels of abstraction, such as the CSF and a research paper on quantum cryptography.
- Subjectively quantify the SOR between elements to provide users with additional insight into the implied bond between reference elements asserted by the developer (SMEs).
- SOR metric score between 1 and 10, 10 being the strongest.
  - For simplicity, we only used 2, 5, and 8 options in our effort

Understand The Mapping: Strength of Relationship (SOR)



A relationship type can encompass relationships of different strengths. Case 1 shows a Focal Document element (f) and a Reference Document element (r) in a Subset relationship with many common elements that would probably have a strength score of 8, while Case 2 shows a Subset relationship where the two elements have fewer common elements that would probably have a strength score of 2.

Understand The Mapping: CSF Core Functions and Categories

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	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
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

The CSF Core has five Functions colored coded and divided into Categories.

The following page further divides the Categories into Subcategories with descriptions.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Understand The Mapping: CSF Core Elements

Function	Category	Subcategory	Samples of Informative Reference
Identify (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	**ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	**ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	**ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	**ISO/IEC 27001:2013** A.11.2.6 **3. NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	**ISO/IEC 27001:2013** A.8.2.1 **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	**ISO/IEC 27001:2013** A.6.1.1 **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11

Understand The Mapping: CIP Reliability Standard Elements

A. Introduction

1. Title: Cyber Security — BES Cyber System Categorization

2. Number: CIP-002-5.1a

B. Requirements and Measures

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

- **i.** Control Centers and backup Control Centers;
- **ii.** Transmission stations and substations;
- **iii.** Generation resources;
- **iv.** Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
- **v.** Special Protection Systems that support the reliable operation of the Bulk Electric System; and
- **vi.** For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and

1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).

Understand The Mapping: CIP Reliability Standard Elements

A. Introduction

1. Title: Cyber Security — Physical Security of BES Cyber Systems

2. Number: CIP-006-6

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in CIP-006-6 Table R1 – Physical Security Plan. [Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].

CIP-006-6 Table R1 – Physical Security Plan	
Part	**Requirements**
1.6	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.
1.8	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.
1.9	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.

Understand The Mapping: CIP Reliability Standard Elements

A. Introduction

1. Title: Cyber Security — Electronic Security Perimeter(s)

2. Number: CIP-005-7

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-7 Table R1 – Electronic Security Perimeter. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].

CIP-005-7 Table R1 – Electric Security Plan	
Part	**Requirements**
1.5	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Understand The Mapping: Mapping CSF Core and CIP Elements

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Comments (optional)	Strength of Relationship (optional)
ID.AM-1	Physical devices and systems within the organization are inventoried	Semantic	superset of	CIP-002-5.1a-R1	R1 Implement a process that considers these assets for parts 1.1 through 1.3 i. Control Centers and backup Control Centers ii. Transmission stations and substations iii. Generation resources iv. Systems for restoration, including Blackstart and Cranking Paths v. Special Protection Systems vi. Specifically identified Distribution Providers, Protection Systems R1.1 Identify high impact BES Cyber Systems, Attachment 1, Section 1 R1.2 Identify medium impact BES Cyber Systems, Attachment 1, Section 2 R1.3 Identify low impact BES Cyber System, Attachment 1, Section 3 (a list not required)	Selected 'Semantic' because elements have similar meanings. Selected 'superset of' because ID.AM-1 is about inventorying all systems, while R1 is about inventorying BES Cyber Systems. Strong relationship strength.	8
PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	Semantic	superset of	CIP-006-6-R1	R1 Implement documented physical security plans that collectively include applicable requirements for Physical Security Plan R1.4 Monitor for unauthorized access into a physical security perimeter R1.5 Issue alarm in response to detected unauthorized access into a physical security perimeter R1.6 Monitor Physical Access Control Systems for unauthorized physical access R1.8 Log entry of authorized individuals into physical security perimeter R1.9 Retain physical access logs for at least ninety calendar days	Selected 'Semantic' because elements have similar meanings. Selected 'superset of' because PR.PT-1 covers all audit/log and R1 covers only physical access. Moderate relationship strength.	5
DE.AE-2	Detected events are analyzed to understand attack targets and methods	Semantic	intersects with	CIP-005-7-R1	R1 Implement documented processes that collectively include the applicable requirements for Electronic Security Perimeter R1.5 Methods for detecting malicious communications for inbound/outbound communications	Selected 'Semantic' because elements have similar meanings. Selected 'intersects with' because R1.5 doesn't specifically discuss analyzing the events, detection technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP. Weak relationship strength.	2

Update The Mapping

- Update the OLIR:
  - NIST will announce that the OLIR is in the process of being updated via a notification in the OLIR Catalog.
  - Major changes will be considered a new submission and will be required to undergo the same review process as a new submission:
    - Changes may require current implementations based on the previous version to be modified
  - Minor changes will undergo a 30-day public comment period:
    - Changes include one or more new relationships without the removal or modification of existing relationships
  - Administrative changes will not have a comment period, and the updated OLIR will be listed in the OLIR Catalog with an appropriate version number to annotate the update:
    - Changes are typographical or stylistic for usability

OLIR Project Sub-Team

- Brent Sessions, SWG Co-Chair, WAPA
- Katherine Street, SWG Co-Chair, Duke Energy
- Aldo Nevárez, Team Lead, WECC
- James Brosnan, WECC
- Monica Jain, SCE
- Michael Johnson, APX
- Jeffrey Marron, NIST
- Karl Perman, EnergySec
- David Vitkus, WECC

Contacts

- Throughout an OLIR's life cycle, any reviewer can submit suggested edits/revisions, comments, or questions to olir@nist.gov. NIST will forward feedback to the developer.

Conclusion

- Described The CSF Core and CIP Reliability Standards
- Explained the Mapping
  - Informative Reference
  - Focal and Reference Documents
  - Focal Elements Map to Reference Elements
  - Rationale Options
  - Relationship Options
  - Strength of Relationship Options
  - Informative Reference Mapping
- Described Process to Update the Mapping

Questions and Answers

National Online Informative References

OLIR DEMO