



# NIST Smart Grid Framework

*NERC CIP and NIST Cybersecurity*

**Avi Gopstein**

Smart Grid Program Manager  
February 24, 2021

### 01. NERC CIP

NERC’s Critical Infrastructure Protection standards provide the foundation for power system security.

### 02. Mapping resource available to all

An updated mapping between the outcomes of the NIST CSF to NERC CIP standards is provided

### 03. How to use it

Understand the relationship between NERC CIP standard (and section) has to the Cybersecurity Framework outcomes

Mapping of CIP Standards to NIST Cybersecurity Framework (CSF) v1.1 Subcategories performed by the same Registered Entity volunteers as samples of "Secure and Compliant"

Category ID	Subcategory	CIP ID	NIST CSF Outcome
1	ID.AM-1: Physical devices and systems within the organization are inventoried	CIP-002-5.1a-R1	CIP-002-5.1a R1: Each Response that considers each of the following through 1.3: i. Control Centers and backup Centers; ii. Transmission stations and substations; iii. Generation resources; iv. Systems and facilities critical to the Bulk Electric System; and v. Special Protection Systems that are critical to the Bulk Electric System; and vi. For Distribution Providers, Protection Systems and Facilities. Applicability section 4.2.1 above 1.1 Identify each of the high impact assets that are critical to the Bulk Electric System, if any; 1.2 Identify each of the medium impact assets that are critical to the Bulk Electric System, if any; 1.3 Identify each asset that could be impacted by a cyber incident according to Attachment 1, Section 2, if any.
1	ID.AM-1: Physical devices and systems within the organization are inventoried	CIP-002-5.1a-R2	CIP-002-5.1a R2: The Responsible Party shall: 2.1 Review the identifications in Attachment 1, Section 1, and update them if there are changes in the system, at least on a calendar monthly basis, even if it has no identified items; 2.2 Have its CIP Senior Management review the identifications required by Requirement R1 at least annually, even if it has no identified items.
2	ID.AM-2: Software platforms and applications within the organization are inventoried	CIP-002-5.1a-R1	CIP-002-5.1a R1: Each Response that considers each of the following through 1.3: i. Control Centers and backup Centers; ii. Transmission stations and substations; iii. Generation resources; iv. Systems and facilities critical to the Bulk Electric System; and v. Special Protection Systems that are critical to the Bulk Electric System; and vi. For Distribution Providers, Protection Systems and Facilities. Applicability section 4.2.1 above 1.1 Identify each of the high impact assets that are critical to the Bulk Electric System, if any; 1.2 Identify each of the medium impact assets that are critical to the Bulk Electric System, if any; 1.3 Identify each asset that could be impacted by a cyber incident according to Attachment 1, Section 2, if any.

# NERC CIP

<https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx>

## Standards for Critical Infrastructure Protection – Version 5(?)

- The NERC Critical Infrastructure Protection standards are in various stages of maturity.
- Some standards are in version 5 (or beyond)
- Other standards are just being introduced



Home > Program Areas & Departments > Standards > CIP Standards

### CIP Standards

Type	Name	Title	Related Information	Status
<b>(CIP) Critical Infrastructure Protection (92)</b>				
<b>Subject to Future Enforcement (5)</b>				
	CIP-005-6	Cyber Security — Electronic Security Perimeter(s)	Related Information	Subject to Future Enforcement
	CIP-008-6	Cyber Security — Incident Reporting and Response Planning		Subject to Future Enforcement
	CIP-010-3	Cyber Security — Configuration Change Management and Vulnerability Assessments	Related Information	Subject to Future Enforcement
	CIP-012-1	Cyber Security — Communications between Control Centers		Subject to Future Enforcement
	CIP-013-1	Cyber Security - Supply Chain Risk Management	Related Information	Subject to Future Enforcement
<b>Subject to Enforcement (11)</b>				
	CIP-002-5.1a	Cyber Security — BES Cyber System Categorization	Related Information	Subject to Enforcement
	CIP-003-8	Cyber Security — Security Management Controls		Subject to Enforcement
	CIP-004-6	Cyber Security - Personnel & Training	Related Information	Subject to Enforcement
	CIP-005-5	Cyber Security - Electronic Security Perimeter(s)	Related Information	Subject to Enforcement
	CIP-006-6	Cyber Security - Physical Security of BES Cyber Systems	Related Information	Subject to Enforcement
	CIP-007-6	Cyber Security - System Security Management	Related Information	Subject to Enforcement
	CIP-008-5	Cyber Security - Incident Reporting and Response Planning	Related Information	Subject to Enforcement
	CIP-009-6	Cyber Security - Recovery Plans for BES Cyber Systems	Related Information	Subject to Enforcement
	CIP-010-2	Cyber Security - Configuration Change Management and Vulnerability Assessments	Related Information	Subject to Enforcement
	CIP-011-2	Cyber Security - Information Protection	Related Information	Subject to Enforcement
	CIP-014-2	Physical Security	Related Information	Subject to Enforcement

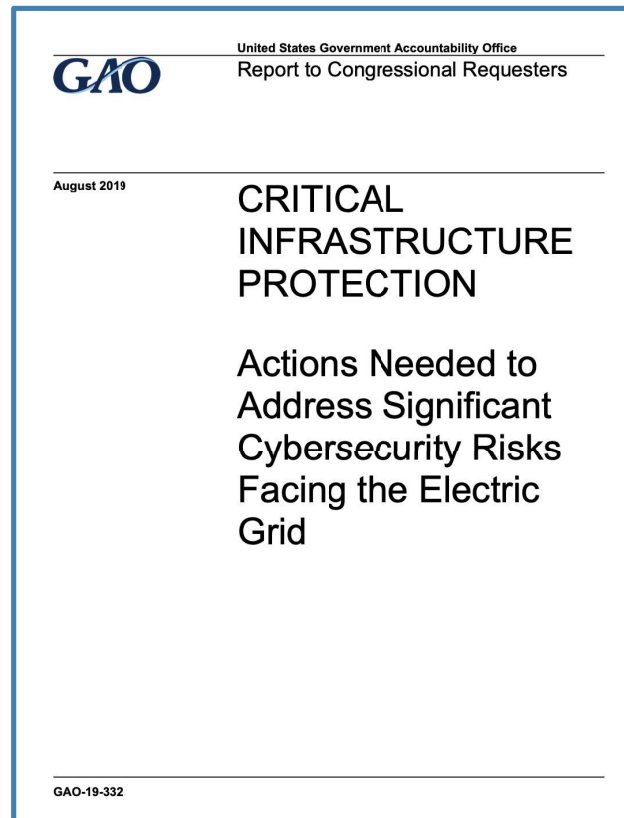
# vs. NIST CSF

## NIST Cybersecurity Framework key to grid security

In 2019, Government Accountability Office urges updates to Nation's power system cybersecurity standards *"to more fully address the NIST Cybersecurity Framework."*

### How to address?

- NIST CSF recently updated (v1.1)
- 5 functions, 23 categories, and 108 subcategories
- 16 NERC CIP standards



GAO is making a recommendation to DOE to develop a plan aimed at implementing the federal cybersecurity strategy for the grid and ensure that the plan addresses the key characteristics of a national strategy, including a full assessment of cybersecurity risks to the grid.

GAO is also making the following two recommendations to FERC:

1. Consider adopting changes to its approved cybersecurity standards to more fully address the NIST Cybersecurity Framework.
2. Evaluate the potential risk of a coordinated cyberattack on geographically distributed targets and, based on the results of that evaluation, determine if changes are needed in the threshold for mandatory compliance with requirements in the full set of cybersecurity standards.

DOE and FERC agreed with GAO's recommendations.

# Mapping: CIP v5, CSF v1.1

<https://www.nerc.com/pa/comp/Pages/CAOneStopShop.aspx>

## A new tool

In July 2020, NERC and NIST released an updated mapping between CIP and CSF

## The latest versions

NIST CSF v1.1 mapped to the latest NERC CIP standards, even those not yet enforced

## Available for everyone

Posted on the NERC CIP “One-Stop Shop” webpage for free download

## Searchable, usable

Excel spreadsheet can be searched and sorted to meet user need and background

The screenshot shows the NERC One-Stop Shop webpage. The left navigation menu includes categories such as Compliance Assurance, Compliance Guidance, Compliance Investigations, Compliance Analysis and Certification, Compliance Hotline, ERO Enterprise Program Alignment Process, Regional Audit Reports of Registered Entities, Risk-Based Compliance Monitoring and Enforcement Program (CMEP), Organization Registration and Organization Certification, Organization Certification, CIP VS Implementation Information, Enforcement and Mitigation, CMEP and Vegetation Reports, Reliability Standards Audit Worksheet (RSAWs), Centralized Organization Registration ERO System (CORES) Technology Project, and Compliance and Certification Committee (CCC). The main content area displays a list of documents under the heading 'One-Stop-Shop (CMEP, Compliance, and Enforcement) - Active'. The list includes 'Compliance (23)' with sub-items like 'CIP ERT & User Guide (3)', 'Compliance (8)', 'Coordinated Oversight (2)', 'Guidance (2)', 'Hotline (1)', 'Implementation Plan (1)', 'Internal Controls (1)', 'Investigations (1)', and 'NIST (1)'. A yellow arrow points to the document 'Mapping of CIP Standards to NIST Cybersecurity Framework (CSF) v1.1' which is listed with a year of 2020, category of NIST, and date of 7/24/2020.

# The Mapping Tool

<https://www.nerc.com/pa/comp/Pages/CAOneStopShop.aspx>

**Mapping of CIP Standards to NIST Cybersecurity Framework (CSF) v1.1 Subcategories performed by Electric Industry Responsible Entity volunteers for NIST and NERC**  
 Guidance language is provided by the same Register of Responsible Entity volunteers as same of "Secure and Compliant" for consideration only, based on a combination of CSF subcategory and CIP Standards

Function	Category	CSF SubCat ID	Subcategory	CIP ID	NERC CIP	CIP Mapping Logic	Guidance for combined NERC CIP and NIST CSF
IDENTIFY (ID)	Asset Management (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	ID.AM-1: Physical devices and systems within the organization are inventoried	CIP-002-5.1a-R1	CIP-002-5.1a R1: Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: 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).	CIP-002-5-1a-R1-1.1 and 1.2 - identify and categorize High and Medium impact BES Cyber Systems and their associated BES Cyber Assets	1. Ensure inventory includes OT and IT physical assets that support reliable operations 2. Must establish a methodology that identifies the Bulk Electric System (BES) Cyber Systems which perform BES reliability operating services (BROS) and evaluate the potential for adverse impact that the loss, compromise, or misuse would have on the reliable operation of the Bulk Electric System (BES).
IDENTIFY (ID)	Asset Management (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	ID.AM-1: Physical devices and systems within the organization are inventoried	CIP-002-5.1a-R2	CIP-002-5.1a R2: The Responsible Entity shall: 2.1 Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and; 2.2 Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.	CIP-002-5-1a-R2 - in defined periods, review identified assets and have a designated Senior Official formally approve	Perform physical asset inventory reviews regularly and compare with previous iterations Results are reviewed by a person with authority to approve
	Asset Management (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-2	ID.AM-2: Software platforms and applications within the organization are inventoried			CIP-002-5-1a-R1 - Identify and categorize BES Cyber Systems and their associated BES Cyber Assets	1. Ensure inventory includes OT and IT all software that support reliable operations

**Navigation:** NIST CSF 1.1 to CIP v5 | CIPv5 to CSF 1.1 XREF | Pivot

# The Mapping Tool

**PivotTable Fields**

- Category
- CSF SubCat ID
- Subcategory
- MII 1

**Filters** **Columns**

**Rows** **Values**

- CIP ID
- CSF SubCat ID

Drag fields between areas

3	Row Labels
4	CIP-002-5.1a-R1
5	CIP-002-5.1a-R2
6	CIP-003-7-R1
7	CIP-003-7-R2
8	CIP-003-7-R3
9	CIP-003-7-R4
10	CIP-003-7-R4
11	CIP-004-6-R1
12	CIP-004-6-R2
13	CIP-004-6-R2
14	CIP-004-6-R3
15	CIP-004-6-R4
16	ID.AM-6
17	PR.AC-1
18	PR.AC-2
19	PR.AC-3
20	PR.AC-4
21	PR.DS-1
22	PR.DS-2
23	PR.DS-5
24	PR.IP-11
25	CIP-004-6-R5
26	CIP-005-5-R1
27	CIP-005-5-R2
28	CIP-005-6 R2
29	CIP-005-6-R2
30	CIP-005-6-R2
31	CIP-006-6-R1
32	CIP-006-6-R2
33	CIP-006-6-R3
34	CIP-007-6-R1
35	CIP-007-6-R2
36	CIP-007-6-R3
37	CIP-007-6-R4

3	Row Labels
4	DE.AE-1
5	No mapping
6	DE.AE-2
7	CIP-003-7-R2
8	CIP-005-5-R1
9	CIP-007-6-R4
10	CIP-008-5-R1
11	CIP-008-5-R2
12	XX-CIP-003-7-R1
13	CIP-008-5-R4
14	DE.AE-3
15	CIP-007-6-R4
16	DE.AE-4
17	CIP-003-7-R2
18	CIP-008-5-R1
19	CIP-008-5-R4
20	DE.AE-5
21	CIP-007-6-R4
22	CIP-007-6-R5
23	CIP-008-5-R1
24	XX-CIP-003-7-R1
25	DE.CM-1
26	CIP-005-5-R1
27	DE.CM-2
28	CIP-003-7-R2
29	CIP-006-6-R1
30	CIP-006-6-R2
31	XX-CIP-014 R4
32	DE.CM-3
33	CIP-006-6-R1
34	CIP-007-6-R4
35	CIP-007-6-R5
36	XX-CIP-003-7-R1
37	DE.CM-4

# Reexamining PR.AC-6

**PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions**

Category	Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power Systems Owners/Operators
	Subcategories				
	PR.AC-5	PR.AC-5	PR.AC-5	PR.AC-5	Network segmentation is an important tool for containing potential incidents (safety, reliability), and limiting damage from incidents (resilience). Grid modernization efforts should consider segmenting networks from the design stage into operations (e.g., DER devices could be segmented to limit exposure to the rest of the power system infrastructure).
	PR.AC-6	PR.AC-6	PR.AC-6	PR.AC-6	In the power system, the safe delivery of reliable power is paramount. For this reason, there may be situations (e.g., emergency maintenance or need to restore power) in which the binding and proofing of credentials may interfere with safety, reliability, and resilience. Power system owners/operators will need to consider any risks introduced if identities are not proofed and bound to credentials and if those credentials are not required for certain user actions.

AutoSave OFF | NIST CSF v1.1 to NERC CIP FINAL

Home | Insert | Draw | Page Layout | Formulas | Data | Review | View | Tell me

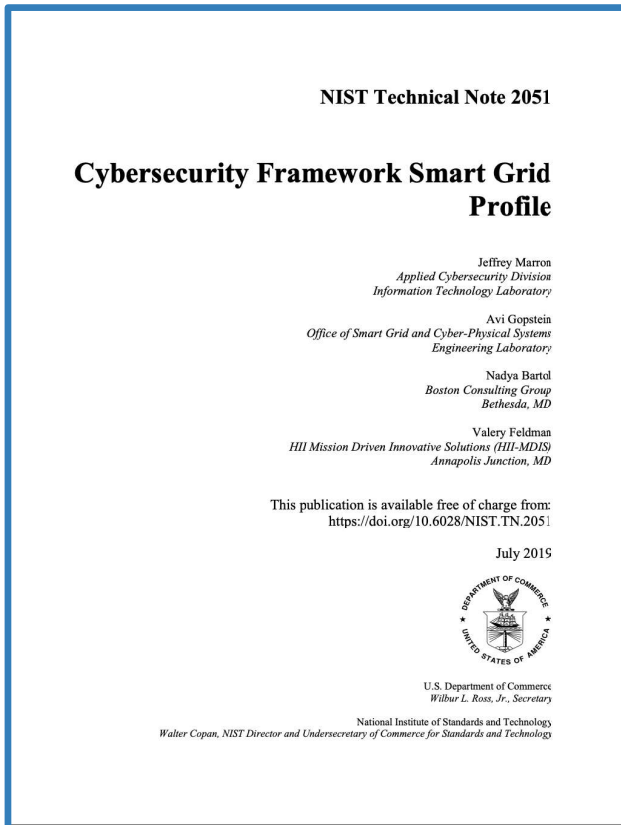
PR.AC-6

Mapping of CIP Standards to NIST Cybersecurity Framework (CSF) v1.1 Subcategories performed by Electric Industry Responsible Entity volunteers, NIST and NERC							
Guidance language is provided by the same Registered Entity volunteers as samples of "Secure and Compliant concepts" for consideration only, based on a combination of CSF subcategory and CIP Standards							
Function	Category	CSF SubCat ID	Subcategory	CIP ID	NERC CIP	CIP Mapping Logic	Guidance for combined NERC CIP and NIST CSF
PROTECT (PR)	Access Control (AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, or devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	PR.AC-5	Network Segregation, Network Segmentation	CIP-007-6-R1	documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R1 – Ports and Services.	Based in Key Information within Standard	Secure network accessible ports as well as physical CIP ports in operation on an asset. This includes monitoring and documenting the status and use of discovered ports.
PROTECT (PR)	Access Control (AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, or devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	PR.AC-6	PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	CIP-004-6-R3	CIP-004-6 R3.1: Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that include 3.1 Process to confirm identity.		CIP-004-6 R3.1 only covers the proof of identity, does not cover the bound to credentials and asserted interactions.
PROTECT (PR)	Access Control (AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, or devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	PR.AC-7	PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	CIP-005-5-R1	CIP-005-5 R1.4: Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.		

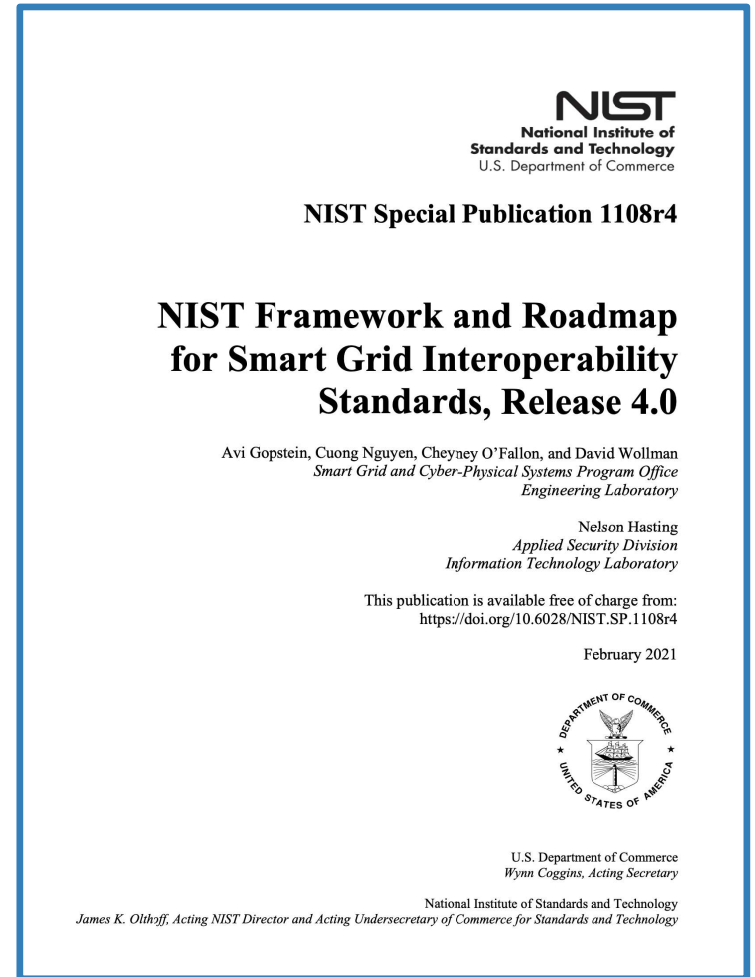
Smart Grid | NIST

*"CIP-004-6 R3 only covers the proof of identity, does not cover the bound to credentials and asserted interactions."*

# Questions?



<https://doi.org/10.6028/NIST.TN.2051>



<https://doi.org/10.6028/NIST.SP.1108r4>