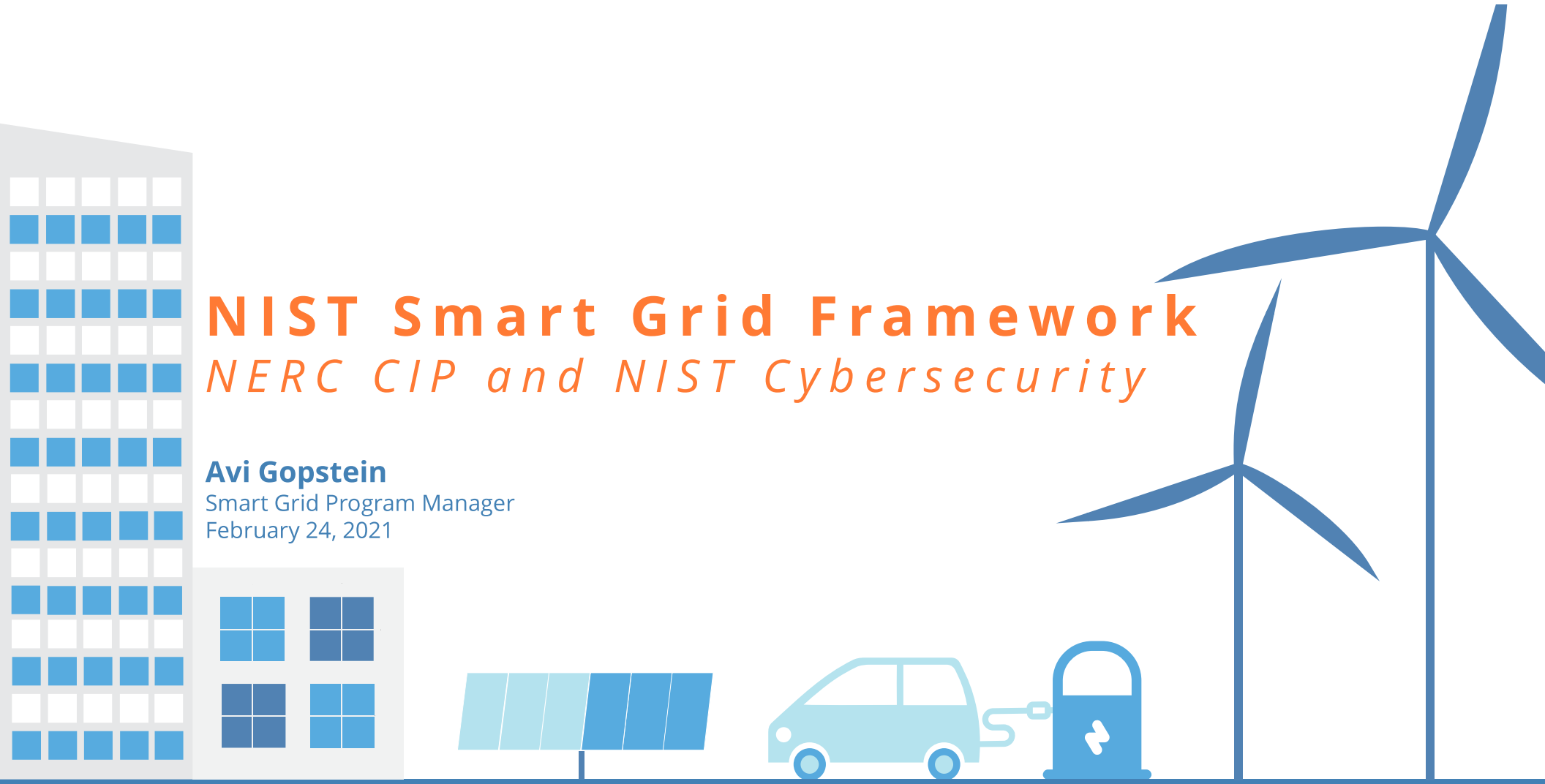
NIST Smart Grid Framework

NERC CIP and NIST Cybersecurity

Avi Gopstein
Smart Grid Program Manager
February 24, 2021



NERC CIP & NIST CSF

01. NERC CIP

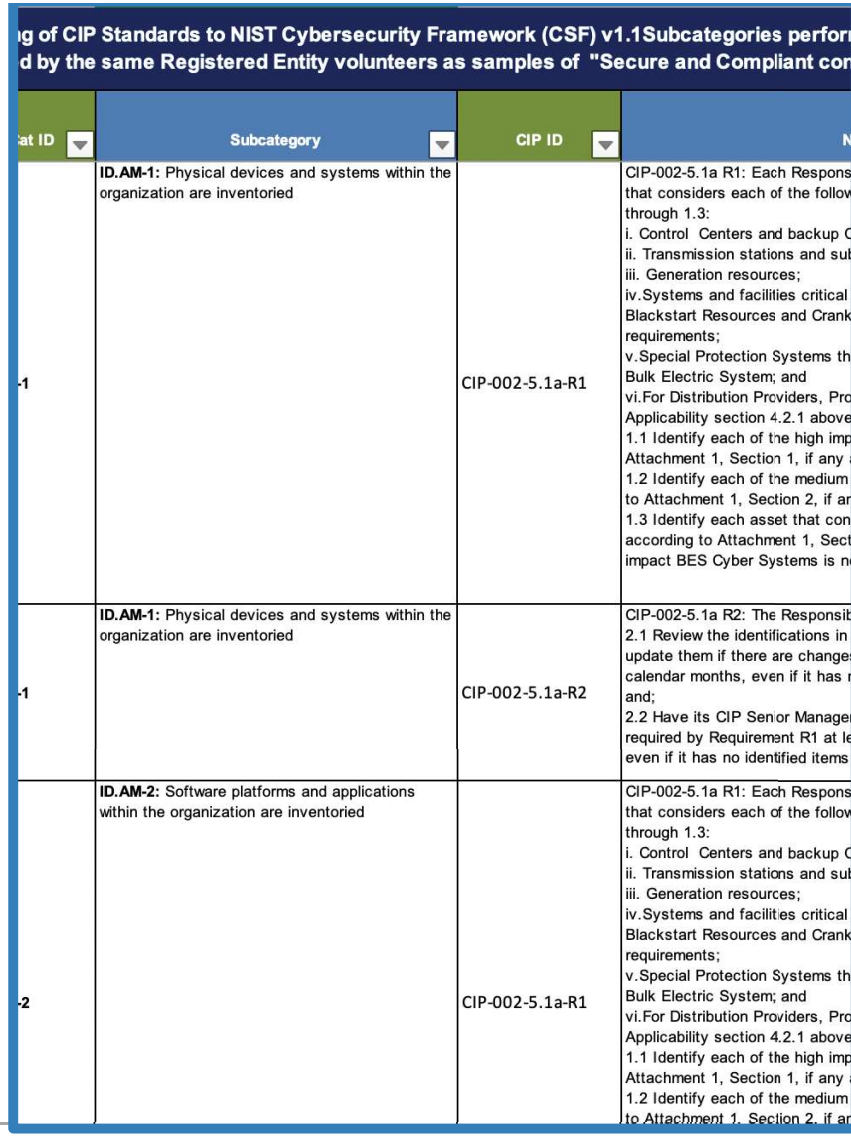
NERC's Critical Infrastructure Protection standards provide the foundation for power system security.

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



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

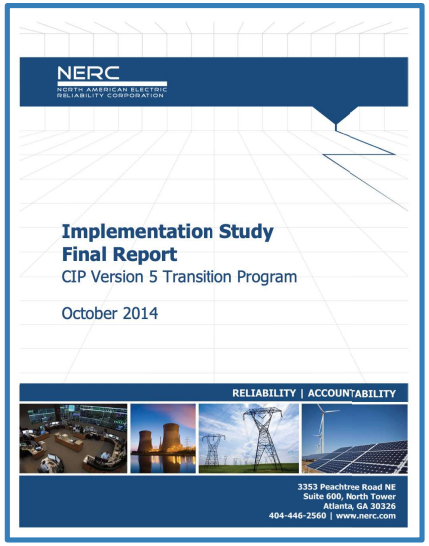
at ID	Subcategory	CIP ID	N
-1	**ID.AM-1:** Physical devices and systems within the organization are inventoried	CIP-002-5.1a-R1	CIP-002-5.1a R1: Each Respons that considers each of the follow through 1.3: i. Control Centers and backup C ii. Transmission stations and sub iii. Generation resources; iv.Systems and facilities critical Blackstart Resources and Crank requirements; v.Special Protection Systems th Bulk Electric System; and vi.For Distribution Providers, Pro Applicability section 4.2.1 above 1.1 Identify each of the high imp Attachment 1, Section 1, if any 1.2 Identify each of the medium to Attachment 1, Section 2, if ar 1.3 Identify each asset that con according to Attachment 1, Sect impact BES Cyber Systems is n
-1	**ID.AM-1:** Physical devices and systems within the organization are inventoried	CIP-002-5.1a-R2	CIP-002-5.1a R2: The Responsib 2.1 Review the identifications in update them if there are changes calendar months, even if it has and; 2.2 Have its CIP Senior Manager required by Requirement R1 at le 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 Respons that considers each of the follow through 1.3: i. Control Centers and backup C ii. Transmission stations and sub iii. Generation resources; iv.Systems and facilities critical Blackstart Resources and Crank requirements; v.Special Protection Systems th Bulk Electric System; and vi.For Distribution Providers, Pro Applicability section 4.2.1 above 1.1 Identify each of the high imp Attachment 1, Section 1, if any 1.2 Identify each of the medium to Attachment 1, Section 2, if ar

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

Reliability Standards

Type	Name	Title	Related Information	Status
	(CIP) Critical Infrastructure Protection (92)			
	Subject to Future Enforcement (5)			
	CIP-005-6	Cyber Security — Electronic Security Perimeter(s)	Related Information	Subject to Future Enforcement
	CIP-008-6	Cyber Security — Incicent 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
	Subject to Enforcement (11)			
	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

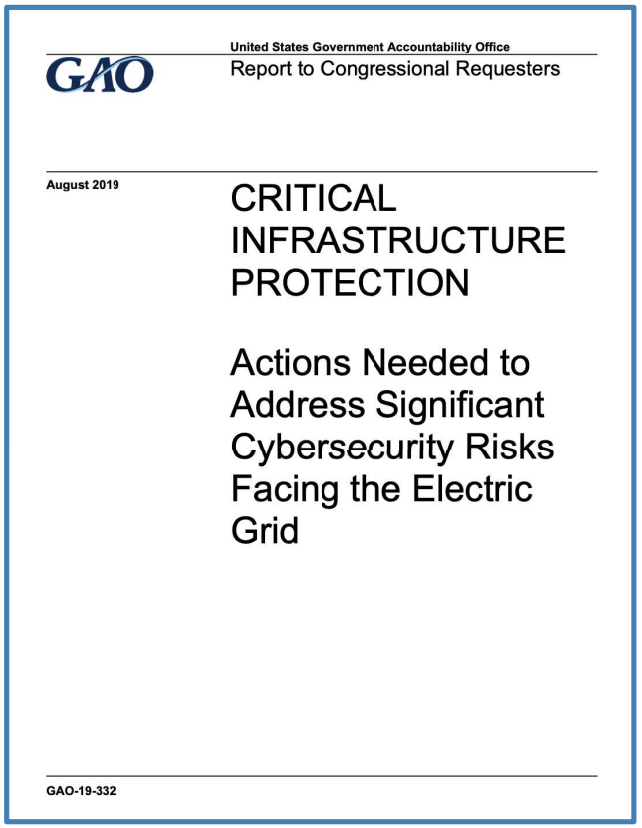
vs. NIST CSF

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

United States Government Accountability Office

Report to Congressional Requesters

August 2019

CRITICAL INFRASTRUCTURE PROTECTION

Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid

GAO-19-332

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

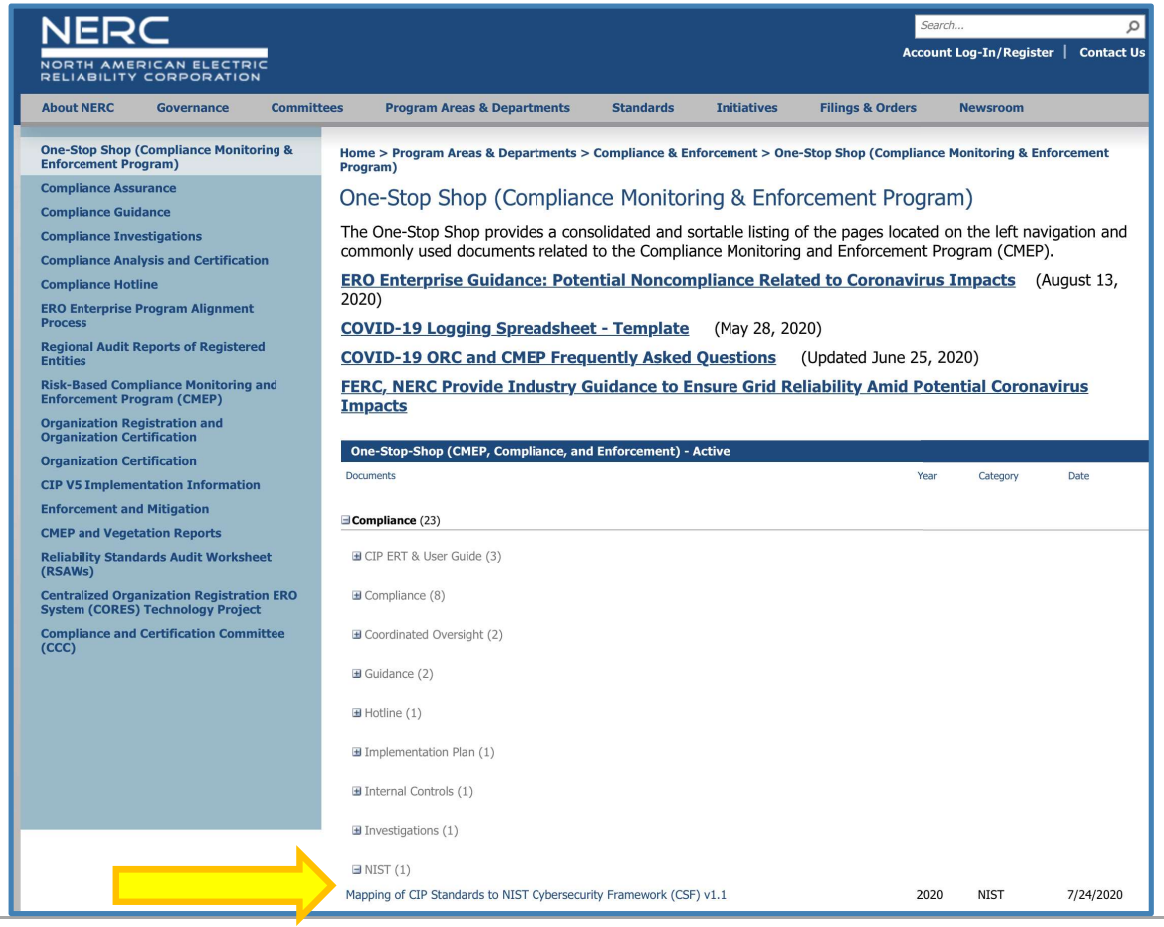
NIST CSF v1.1 mapped to the latest NERC CIP standards, even those not yet enforced

Available for everyone

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

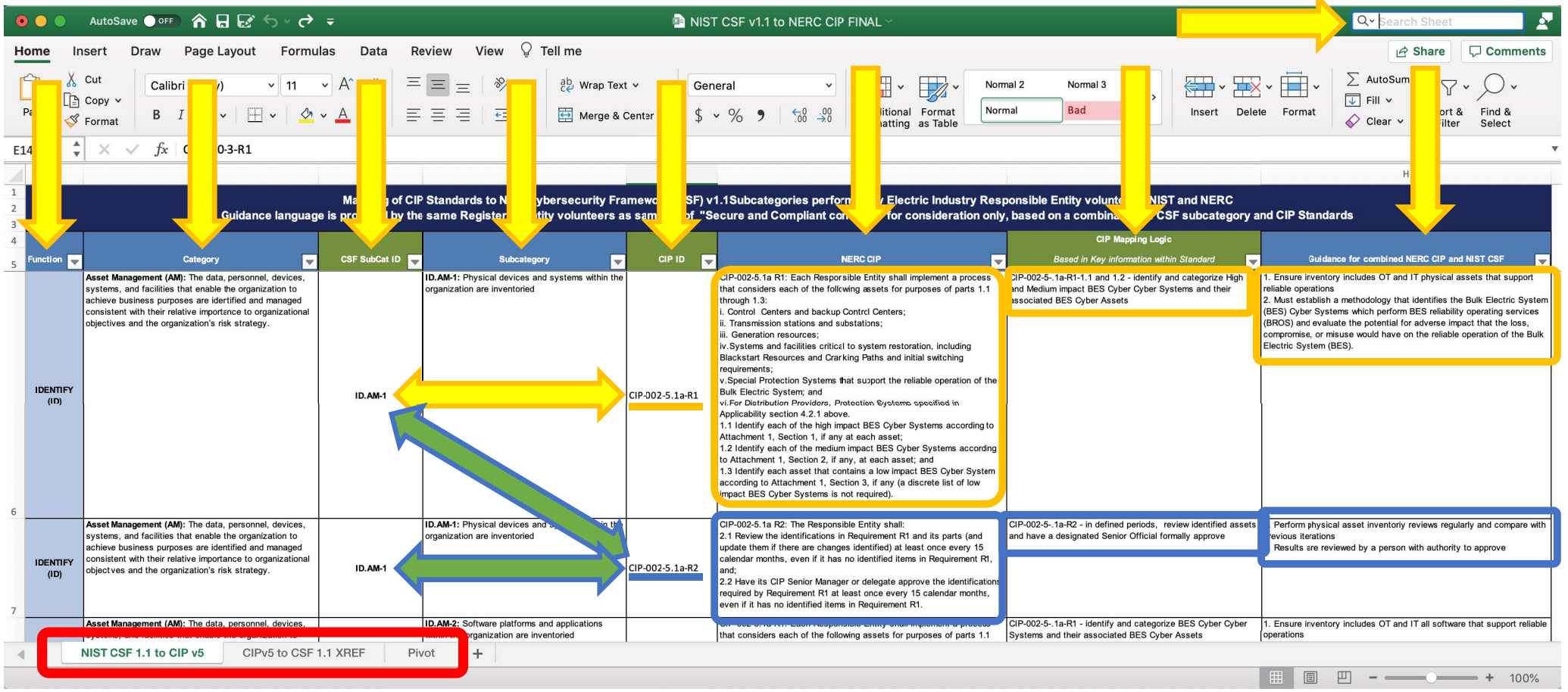
Searchable, usable

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

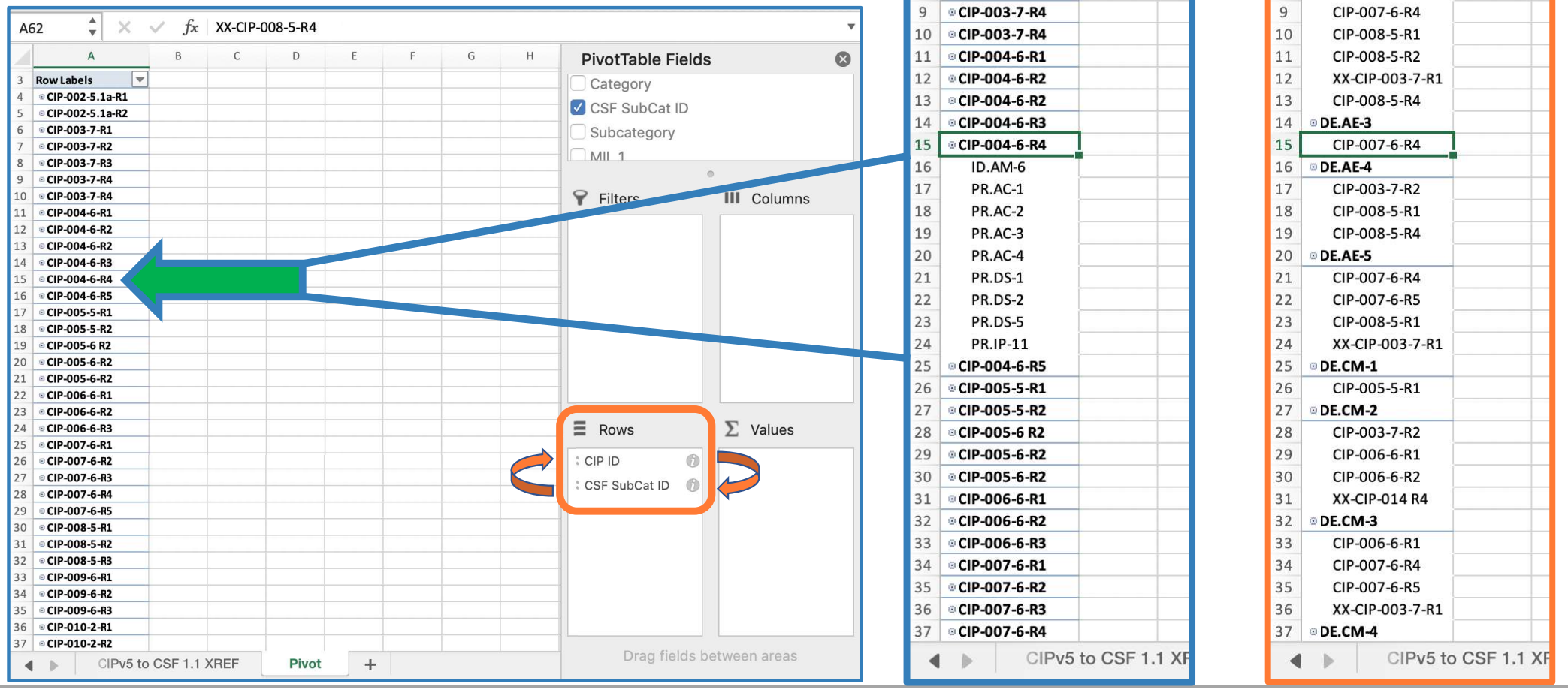


The Mapping Tool

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



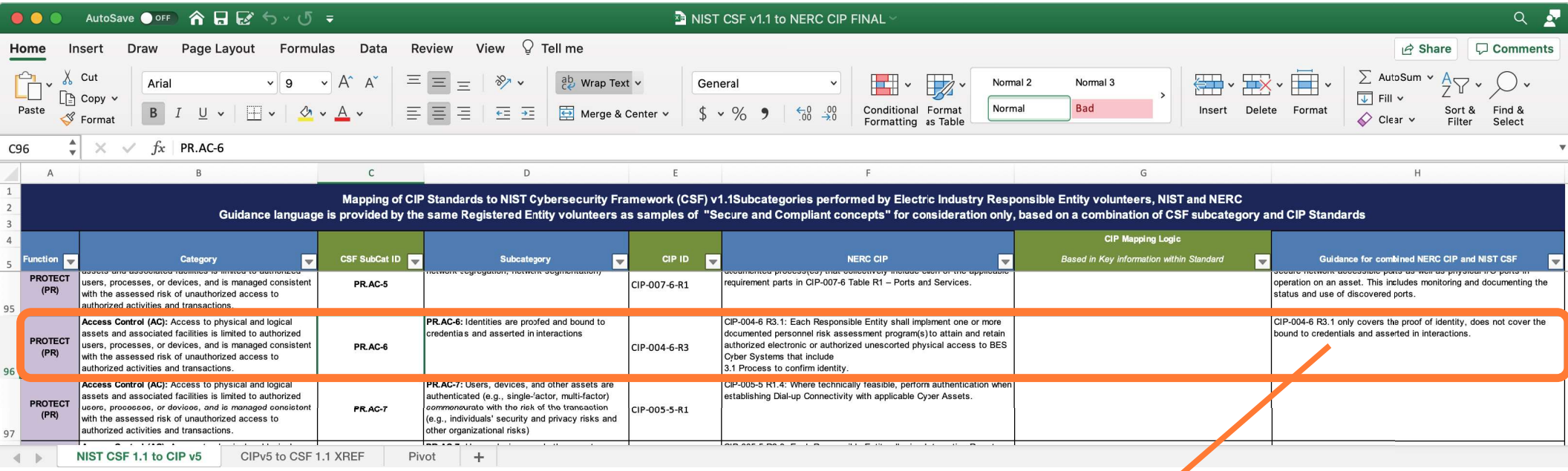
The Mapping Tool



Reexamining **PR.AC-6**

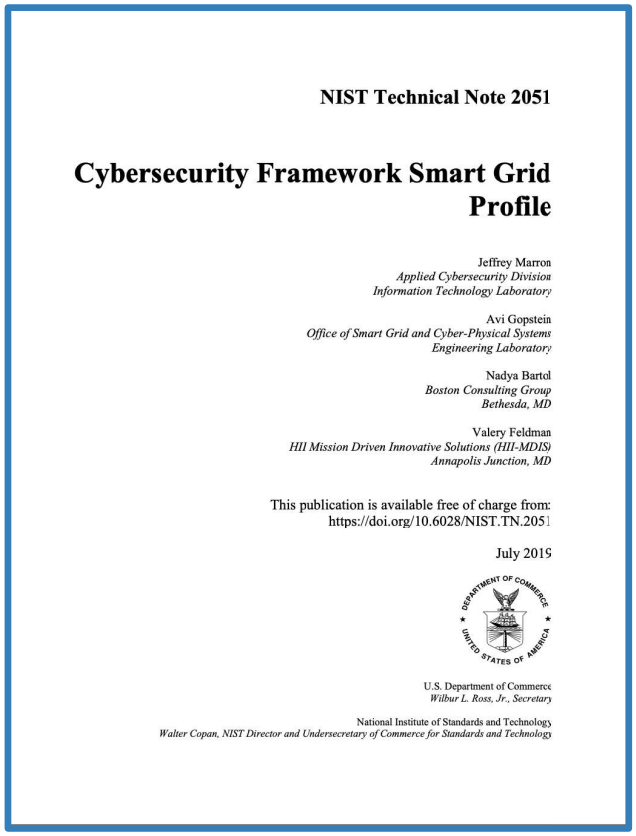
PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power Systems Owners/Operators
Category		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.



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

Questions?



NIST Technical Note 2051

Cybersecurity Framework Smart Grid Profile

Jeffrey Marron
Applied Cybersecurity Division
Information Technology Laboratory

Avi Gopstein
Office of Smart Grid and Cyber-Physical Systems
Engineering Laboratory

Nadya Bartol
Boston Consulting Group
Bethesda, MD

Valery Feldman
HII Mission Driven Innovative Solutions (HII-MDIS)
Annapolis Junction, MD

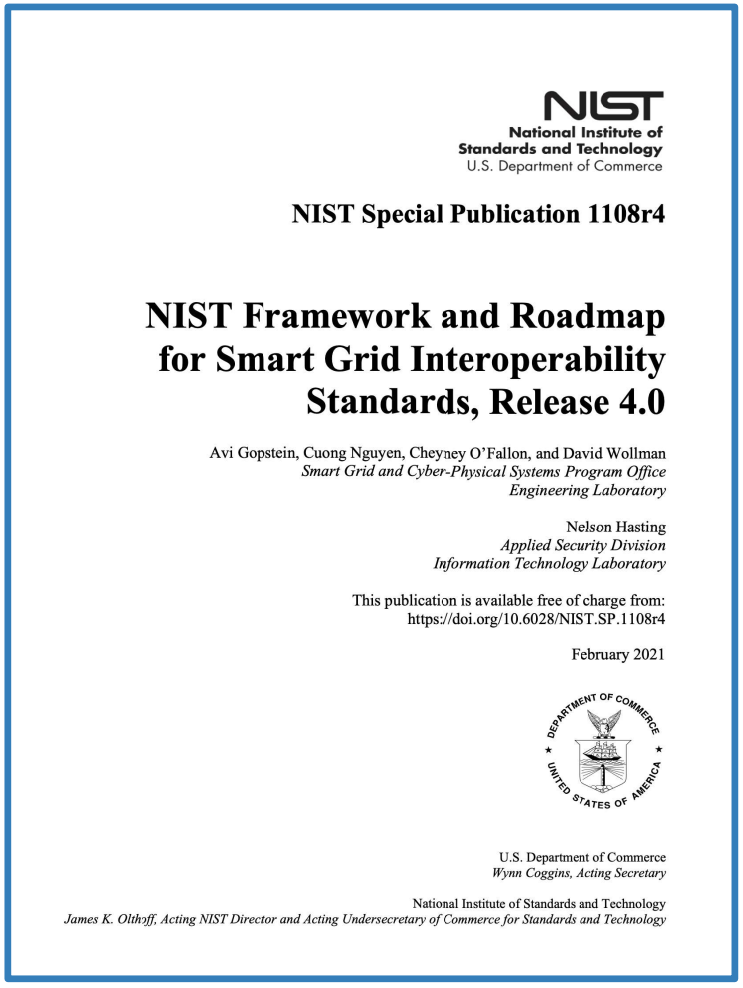
This publication is available free of charge from:
https://doi.org/10.6028/NIST.TN.2051

July 2019

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Undersecretary of Commerce for Standards and Technology

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



NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST Special Publication 1108r4

NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0

Avi Gopstein, Cuong Nguyen, Cheyney O'Fallon, and David Wollman
Smart Grid and Cyber-Physical Systems Program Office
Engineering Laboratory

Nelson Hasting
Applied Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1108r4

February 2021

U.S. Department of Commerce
Wynn Coggins, Acting Secretary

National Institute of Standards and Technology
James K. Olthoff, Acting NIST Director and Acting Undersecretary of Commerce for Standards and Technology

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