NIST Smart Grid Framework

Securing Organizations

Avi Gopstein
Smart Grid Program Manager
February 24, 2021

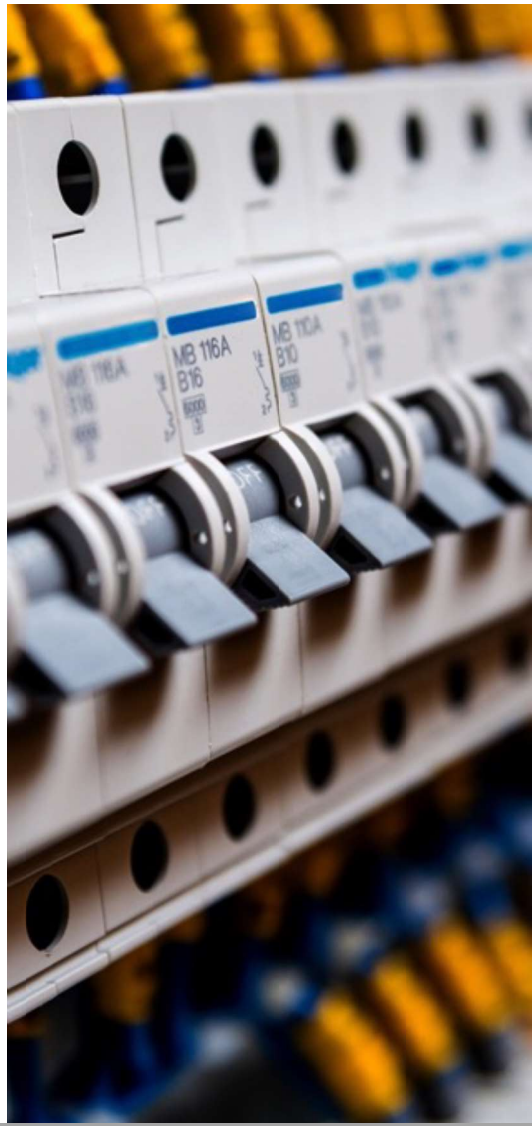
Securing Organizations

1. The NIST Cybersecurity Framework

Helps organizations prioritize their cybersecurity activities.

2. Smart Grid Profile for Cybersecurity

Provides grid-focused context for outcomes described in the Cybersecurity Framework.



1. The Framework Core

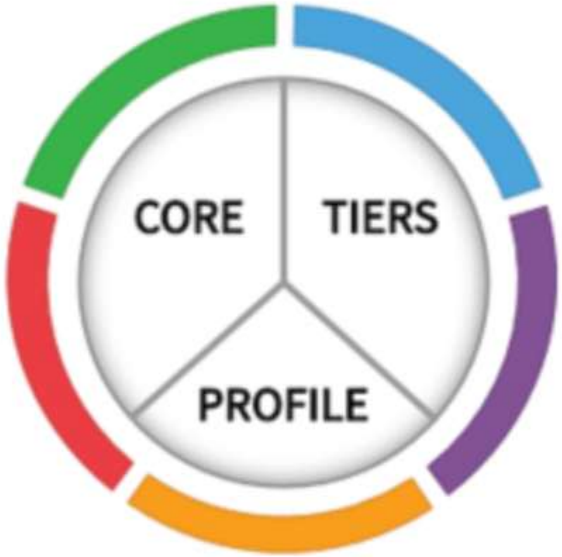
Establishes a common language for evaluating cybersecurity

2. Functions and Categories

Breaking down the five functions needed to keep a system secure

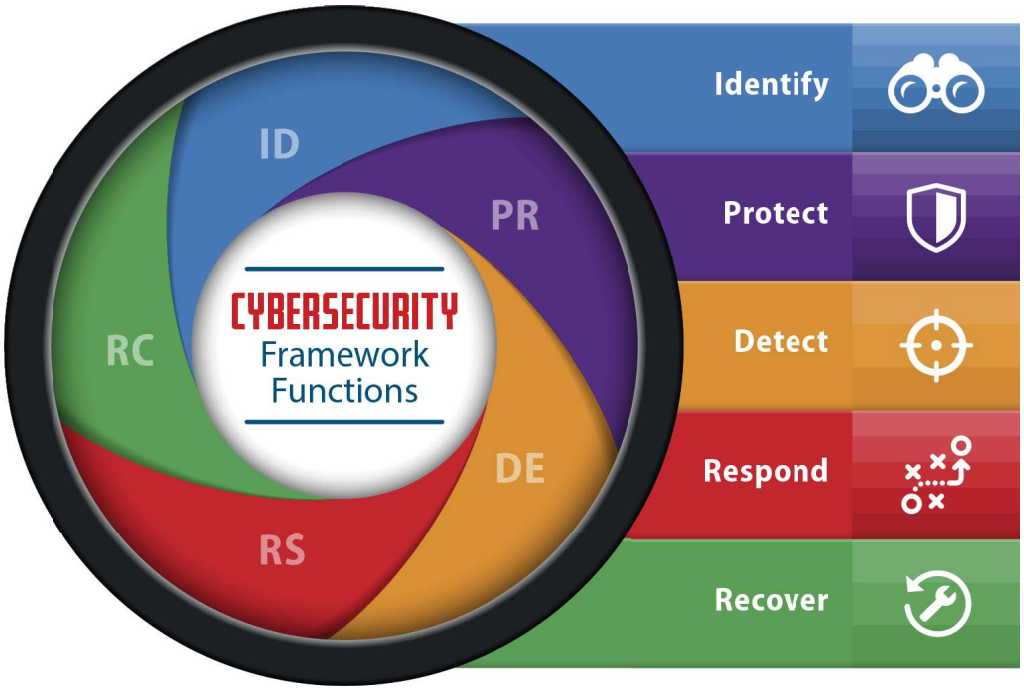
3. Subcategories and references

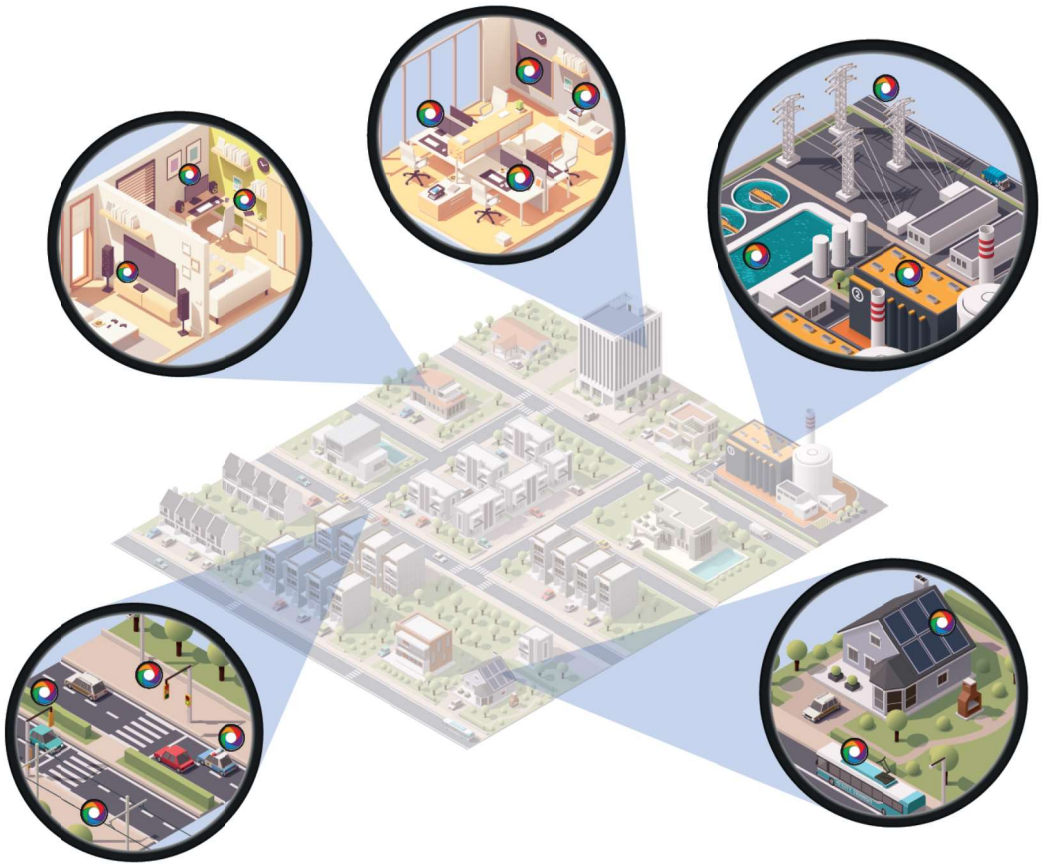
Helping you determine how you can protect your organization



https://www.nist.gov/cyberframework

Framework Core: **Functions**





Framework Core: **Functions and Categories**

	Function	Category
What processes and assets need protection?	**Identify**	Asset Management
		Business Environment
		Governance
		Risk Assessment
		Risk Management Strategy
		Supply Chain Risk Management[1.1]
What safeguards are available?	**Protect**	**Identity Management, Authentication and Access Control**[1.1]
		Awareness and Training
		Data Security
		Information Protection Processes & Procedures
		Maintenance
		Protective Technology
What techniques can identify incidents?	**Detect**	Anomalies and Events
		Security Continuous Monitoring
		Detection Processes
What techniques can contain impacts of incidents?	**Respond**	Response Planning
		Communications
		Analysis
		Mitigation
		Improvements
What techniques can restore capabilities?	**Recover**	Recovery Planning
		Improvements
		Communications

Framework Core: **Subcategories and References**

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

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **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** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

https://www.nist.gov/cyberframework/online-learning/components-framework

Framework Core: **Subcategories & References**

Function	Category	Subcategory	Informative References
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	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **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	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **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

5 Functions 23 Categories 108 Subcategories 6 Informative References

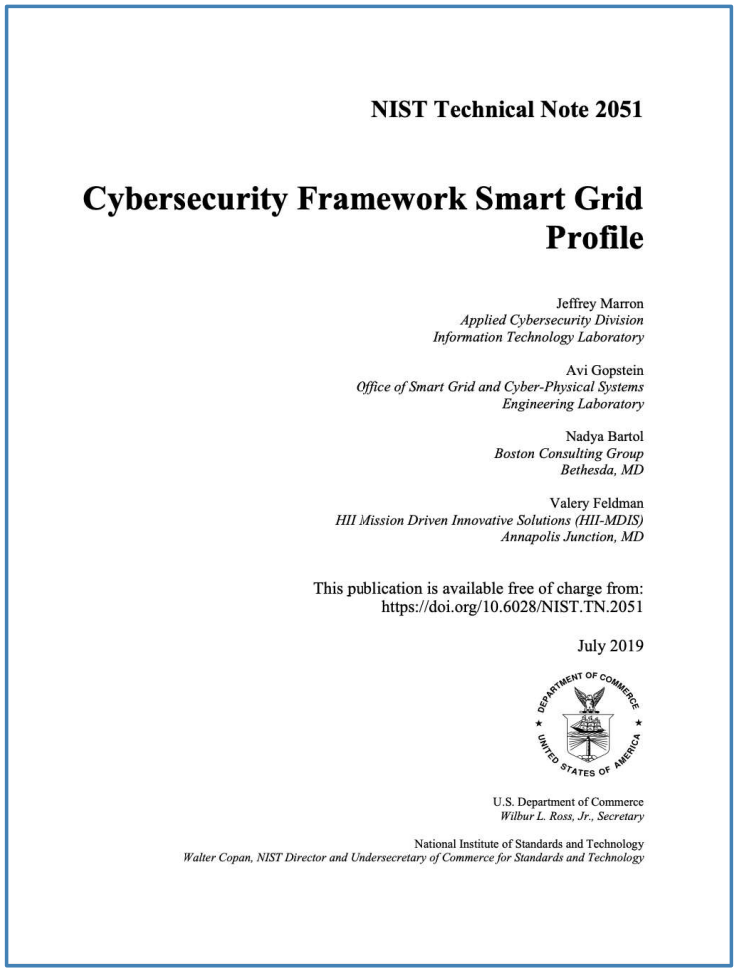
Smart Grid Profile

1. Business objectives

Cybersecurity outcomes are evaluated against their impact on stated business objectives

2. Considerations

A description of the issues that are considered in assessing each subcategory outcome



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

Smart Grid Profile: **Business Objectives**

1. **Maintain safety**
2. **Maintain power system reliability**
3. **Maintain power system resilience**
4. **Support grid modernization**

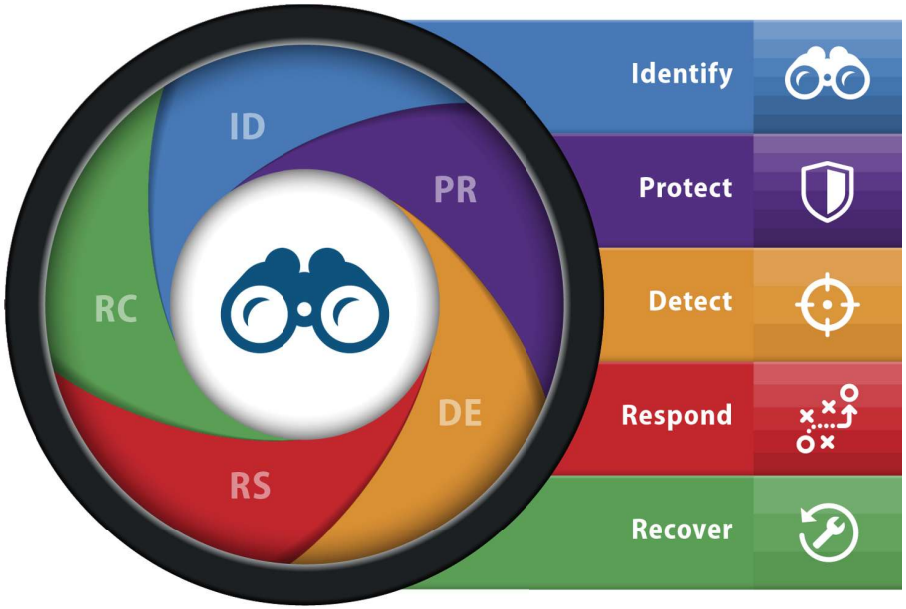
Smart Grid Profile: **Considerations**

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power Systems Owners/Operators
Category		**Subcategories**				
	Access Control	PR.AC-1	PR.AC-1	PR.AC-1	PR.AC-1	Identity management is essential for all users, devices, and processes in both traditional and modernized environments.
		PR.AC-2	PR.AC-2	PR.AC-2	PR.AC-2	Power system owners/operators should control physical access to the power system components as needed, including modernized and distributed grid components. Power system owners/operators should consider the limitations of maintaining physical access to devices on other premises, especially those devices that are owned by a 3rd party.
PR		PR.AC-3	PR.AC-3	PR.AC-3	PR.AC-3	Many grid components are maintained remotely and such remote access should be secured. For modernized environments, consider the limitations of managing remote access to devices that are owned by a 3rd party, such as distributed resources.
		PR.AC-4	PR.AC-4	PR.AC-4	PR.AC-4	Least privilege is important for limiting permissions and authorizations to manage connected devices. This reduces risks of unapproved operations which may create negative impacts to safety, reliability, and resilience. For example, excessive privileges may create an opportunity for compromise during power restoration. Grid modernization efforts should ensure that least privilege principles are designed into and implemented in the modernized grid.

Smart Grid Profile: **Considerations**

		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.

PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	· **CIS CSC**, 16 · **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 · **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 · **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 · **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3

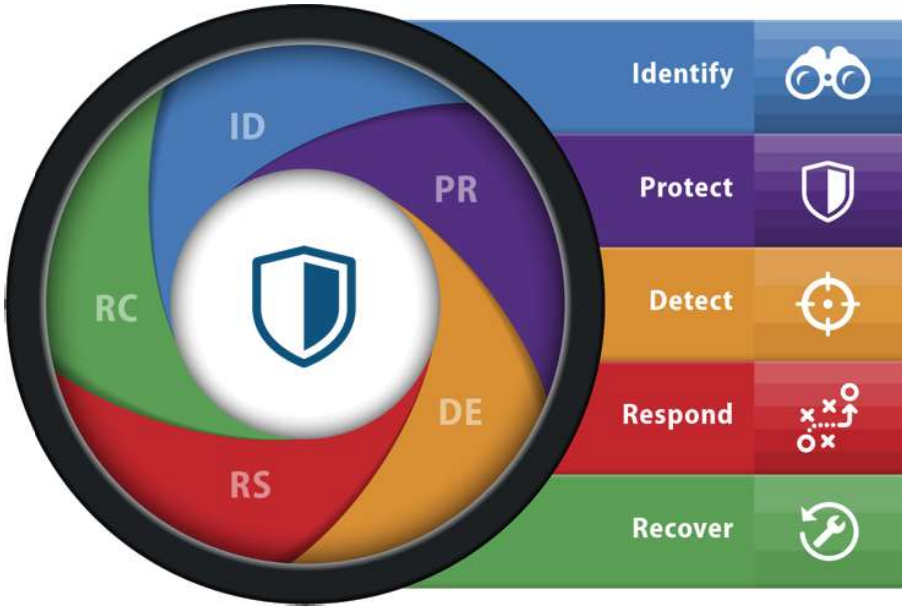


	Category	Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power System Owners/Operators
		Subcategories				
		ID.GV-1	ID.GV-1	ID.GV-1	ID.GV-1	Information security policy drives a set of coherent security requirements throughout the organization. In this context, security policy should support safety, reliability, resilience, privacy, and other related concerns. Also within this context, grid components are cyber-physical systems (CPS) themselves, composed into a more complex, networked cyber-physical system of systems. The NIST CPS Public Working Group (PWG) Framework provides a set of relevant concerns. Organizational informational security policy should address OT and IT environments and how they integrate, the complexity of external partnerships, as well as cover both traditional and modernized environments.
	Governance	ID.GV-2	ID.GV-2	ID.GV-2	ID.GV-2	Information security roles and responsibilities and their coordination with external partners directly affect all requirements. In the context of the modernized grid, external parties include the owners of distributed resources.
		ID.GV-3	ID.GV-3	ID.GV-3	ID.GV-3	Legal and regulatory requirements regarding cybersecurity are especially applicable in the highly regulated critical infrastructure environment of electric power generation, transmission, and distribution. The modernized grid has additional regulatory requirements that should be considered here.
		ID.GV-4	ID.GV-4	ID.GV-4	ID.GV-4	Because the grid is a large cyber-physical system, governance and risk management processes should address all risks, not just cybersecurity.
	Risk Assessment	ID.RA-1	ID.RA-1	ID.RA-1	ID.RA-1	Identifying and documenting asset vulnerabilities can be performed as part of a risk assessment. Vulnerabilities from traditional and modernized environments should be included, especially cyber-physical devices in the modern grid.

Governance:
The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk

ID.GV-2:
Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.

Considerations for Smart Grid:
Information security roles and responsibilities and their coordination with external partners *directly affect all requirements*. In the context of the modernized grid, *external parties include the owners of distributed resources.*

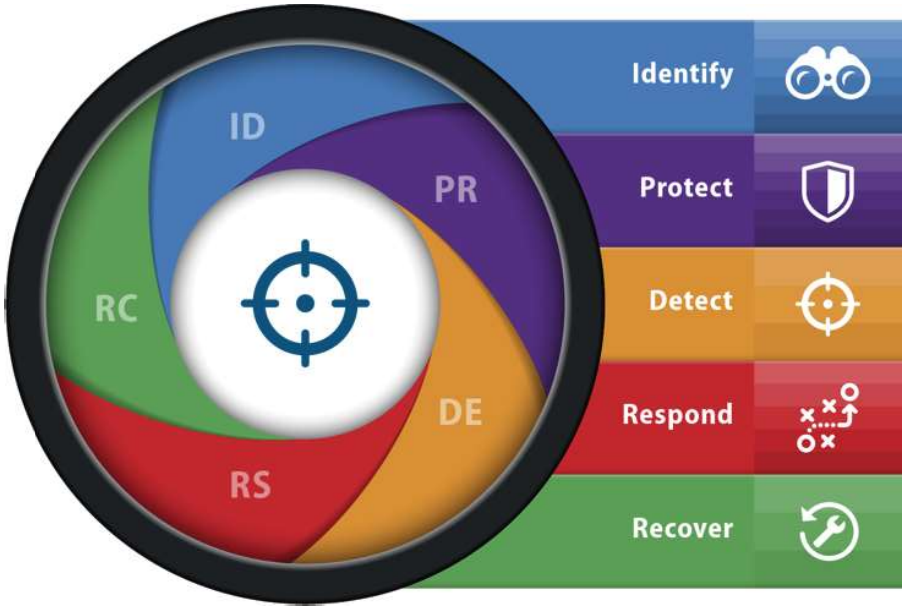


		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power Systems Owners/Operators
	Category					
		PR.DS-1	PR.DS-1	PR.DS-1	PR.DS-1	n the case of power grid systems, protecting data-at-rest ould apply to protecting the integrity of device settings. If mpered with, device settings may cause a safety or reliability sue.
	Data Securit	PR.DS-2	PR.DS-2	PR.DS-2	PR.DS-2	the case of power grid systems, protecting data in-transit is important tool to help protect the integrity of control formation and device settings. Loss of integrity of control formation may cause a safety or reliability issue. Power stem owners/operators should consider the potential for source-intensive cryptographic mechanisms to interfere with e functional performance of control systems and use ditional methods to protect data in transit when less source intensive cryptographic mechanisms are used.
		PR.DS-3	PR.DS-3	PR.DS-3	PR.DS-3	wer system owners/operators neec to be aware of all stributed, modernized assets they own and manage them roughout the life cycle. IT components embedded in OT vices within the grid modernization infrastructure (e.g., wer control and delivery) may present challenges of vnership/contractual agreements with the manufacturers. uring disposal of assets, special care should be taken to not pose device configuration data. The integrity of device nfiguration data should be protected to not impact future afety and reliability.
		PR.DS-4	PR.DS-4	PR.DS-4	PR.DS-4	Understanding capacity requirements is critical for power system reliability and resilience.

Data Security:
Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information

PR.DS-1:
Data-at-rest is protected

Considerations for Smart Grid:
In the case of power grid systems, protecting data-at-rest should apply to protecting the integrity of device settings. If tampered with, device settings may cause a safety or reliability issue.



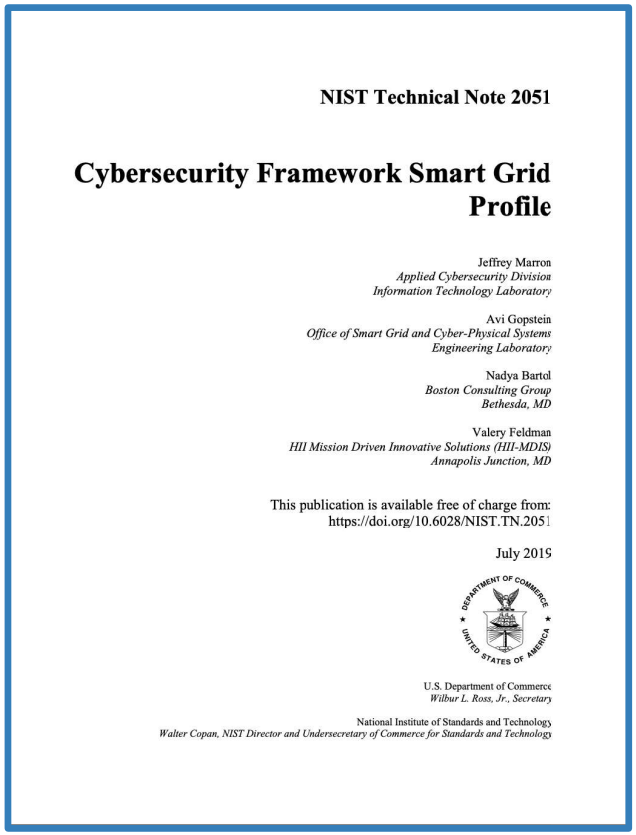
		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power Systems Owners/Operators
	Category	Subcategories				
DE		DE.AE-1	DE.AE-1	DE.AE-1	DE.AE-1	A baseline of network operations and expected data flows is extremely important in the OT context because information flows are predictable, and control systems generally have few users. Understanding the control information flows will help monitor and detect unusual network behavior and allow for timely response. This applies to both traditional and modernized grid environments.
DE	Anomalies and Events	DE.AE-2	DE.AE-2	DE.AE-2	DE.AE-2	Analyzing detected cybersecurity events is critical for safety, reliability, and resilience. There are no special considerations for modernized parts of the infrastructure.
DE	Anomalies and Events	DE.AE-3	DE.AE-3	DE.AE-3	DE.AE-3	When collecting and aggregating data from third-party devices, the devices and the data should be authenticated and validated. Without this authentication and validation, power system owners/operators should carefully consider whether those devices and their data can be trusted.
DE	Anomalies and Events	DE.AE-4	DE.AE-4	DE.AE-4	DE.AE-4	Determining the impact of detected cybersecurity events is critical for safety, reliability, and resilience. There are no special considerations for modernized parts of the infrastructure.
DE	Anomalies and Events	DE.AE-5	DE.AE-5	DE.AE-5	DE.AE-5	Establishing incident alert thresholds is critical for safety, reliability, and resilience. This practice applies to both traditional and modernized parts of the grid.

Anomalies and Events:
Anomalous activity is detected and the potential impact of events is understood

PR.DS-1:
A baseline of network operations and expected data flows for users and systems is established and managed

Considerations for Smart Grid:
A baseline of network operations and expected data flows is extremely important in the OT context because information flows are predictable, and control systems generally have few users. Understanding the control information flows will help monitor and detect unusual network behavior and allow for timely response. This applies to both traditional and modernized grid environments.

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

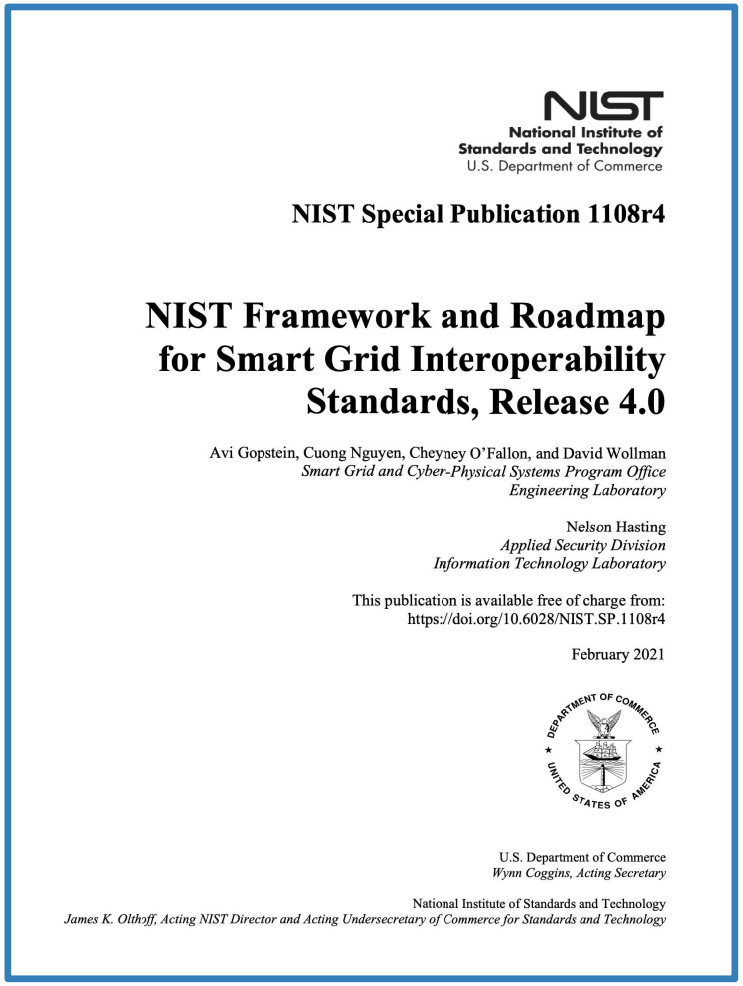
This publication is available free of charge from:
https://doi.org/10.6028/NIST.TN.2051

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