CYBERSECURITY BASELINES FOR ELECTRIC DISTRIBUTION SYSTEMS AND DER

JANUARY 2025

Interim Implementation Guidance: **Scope and Prioritization of the Baselines**

Cybersecurity Baselines for Electric Distribution Systems and DERs-

Interim Implementation Guidance: Scope and Prioritization of the Cybersecurity Baselines

Table of Contents

Note on Usage:

This interim guidance provides a companion document to the *Cybersecurity Baselines for Electric Distribution Systems and DER*. Discussions of individual baselines herein should reference the full content of the baselines in that document. This guidance represents an interim draft that may be modified and expanded by the Steering Group in the final guidance.

Disclaimer

This material is based upon work supported by the Department of Energy under Award Number DE-CR0000009.

Acknowledgements

Steering Group and Tiger Team Participants

Thank you to the following organizations for their contributions, review, and comments to inform the contents of this document.

1898 & Co. | Part of Burns & McDonnell
American Public Power Association (APPA)
Ampyx Cyber
Arkansas Public Service Commission
Bridgette Bourge Security LLC
City Utilities of Springfield
CNK Solutions
ConEdison
Cybersecurity and Infrastructure Security Agency (CISA)
Dominion Energy Services
Duke Energy
Edison Electric Institute (EEI)
Electric Power Research Institute (EPRI)
Excel Energy
Exelon
GE Vernova
Guidehouse
Idaho National Laboratory (INL)
Illinois Commerce Commission
Indiana Regulatory Utility Commission
Massachusetts Department of Public Utilities
Minnesota Department of Commerce, Office of Energy Reliability and Security
Missouri Office of the Public Counsel
National Association of State Energy Offices (NASEO)
National Energy Renewable Laboratory (NREL)
Nebraska Public Power District
New Jersey Board of Public Utilities
NextEra Energy
North Dakota Public Service Commission
Office of New York State Governor
Protect Our Power
Public Service Commission of the District of Columbia
Public Utility Commission of Texas
SANS Institute
Schneider Electric
Solar Energy Industries Association (SEIA)
SolarEdge Technologies
Sungrow
SunSpec Alliance
Virginia State Coorporation Commission
Washington State Department of Commerce, Energy Resilience & Emergency Management Office
Xanthus Consulting
Xcel Energy

U.S. Department of ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

U.S. Department of Energy (DOE)

The Department of Energy (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) leads the Sector Risk Management Agency (SRMA) work on behalf of DOE for the Energy Sector. In this role, CESER is responsible for coordinating risk management activities to help the sector assess and mitigate energy sector critical infrastructure risk. This Cybersecurity Baselines effort is a product of DOE's SRMA responsibilities, providing the sector with voluntary guidance to help them mitigate the cyber risk of the electric distribution system and distributed energy resources (DER). DOE is not a regulator and partners with the private sector and state officials in a voluntary capacity, to provide open communication and information. Visit ***energy.gov/ceser/***

NARUC
National Association of Regulatory Utility Commissioners

National Association of Regulatory Utility Commissioners (NARUC)

NARUC is a non-profit organization founded in 1889 whose members include the governmental agencies that are engaged in the regulation of utilities and carriers in the fifty states, the District of Columbia, Puerto Rico and the Virgin Islands. NARUC's member agencies regulate telecommunications, energy, and water utilities. NARUC represents the interests of state public utility commissions before the three branches of the federal government.

Direct comments and questions on this publication to *cyberbaselines@naruc.org*.

Introduction

The U.S. electric distribution system is essential to delivering the energy that powers the nation's economy, public safety, and national security. But the grid is changing fast as technology evolves and the demand for energy becomes greater and more variable. The convergence of information technology (IT) and operational technology (OT) systems has given owners and operators more flexibility and greater efficiencies but also increased the complexity of the technology underlying the grid. Meanwhile, consumers, businesses, and industry are adopting a multitude of distributed energy resources (DERs)—at increasingly significant scales—that store or produce energy and enable controllable loads. These changes make the distribution grid more flexible, adaptable, and resilient but also fundamentally change how digital risks must be mitigated in the distribution system.

Given its critical nature, nation-state adversaries actively target the energy sector, as evidenced by the actions of advanced persistent threat actor Volt Typhoon, a group affiliated with the People's Republic of China, who compromised U.S. critical infrastructure systems, including within the energy sector, to position themselves to disrupt those systems in the event of conflict with the United States and its allies.[1] A successful cyber attack could result in physical consequences that disrupt power and initiate prolonged cascading and debilitating impacts on national security, economic security, and public health or safety.

Safeguarding the electric power grid is a responsibility shared by federal, state, local, tribal, and territorial entities, and public and private owners and operators alike. Each of these stakeholders have a unique role to play in the protection of the nation's energy infrastructure.

Protecting the Electric Distribution Grid without a Patchwork Approach

The growing importance of cybersecurity for the electric power grid has led to the creation of myriad cybersecurity frameworks, standards and regulations, including the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards.[2] This set of federally mandated requirements is designed to protect the North American power grid and includes common cybersecurity controls such as asset identification, access control, and incident response. NERC CIP standards, however, only apply to the bulk electric system (BES),[3] and do not apply to the electric distribution system—which is under state, municipal, or cooperative jurisdiction—or to DERs.

States have recognized that gap at the distribution level and are moving quickly to fill it. A state-by-state approach to cybersecurity for the distribution grid, however, may introduce inconsistencies and added complexity for owners and operators—many of whom manage distribution system assets in more than one state. A patchwork approach where states implement bespoke requirements would be more costly for owners and operators and their ratepayers.

Cybersecurity Baselines for Electric Distribution Systems and DERs and Implementation Guidance

Recognizing the lack of uniform cybersecurity standards across the distribution system and the growing cyber threat, the U.S. Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) partnered with the National Association of Regulatory Utility Commissioners (NARUC) to create the *Cybersecurity Baselines for Electric Distribution Systems and DERs*. These risk-based Cybersecurity Baselines are a non-prescriptive set of minimum cybersecurity controls for distribution systems and DERs. They may be used by regulatory bodies and distribution system asset owners and operators as a potential framework for developing their own cybersecurity requirements.

States that choose to adopt the Cybersecurity Baselines will be aligned in their approach to mitigate cybersecurity risk and enhance electric grid security. Common cybersecurity requirements applied consistently across states will harmonize efforts to protect the distribution grid, minimize potential security gaps or overlaps, and reduce the potential costs that owners and operators would incur in meeting multiple, inconsistent requirements.

1. U.S. Cybersecurity and Infrastructure Security Agency, U.S. Department of Energy, and partners, "PRC State-Sponsored Cyber Activity: Actions for Critical Infrastructure Leaders," joint fact sheet, March 2024, *https://www.cisa.gov/sites/default/files/2024-03/Fact-Sheet-PRC-State-Sponsored-Cyber-Activity-Actions-for-Critical-Infrastructure-Leaders-508c_0.pdf*.
2. CIP standards are issued by NERC and enforced under the oversight of the Federal Energy Regulatory Commission (FERC). See: NERC, "Reliability Standards: (CIP) Critical Infrastructure Protection," *https://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx*.
3. The bulk electric systems includes transmission assets operated or connected at 100 kV or higher. See: NERC, Glossary of Terms Used in NERC Reliability Standards, last updated January 7, 2025, *https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf.*

About this Interim Implementation Guidance

NARUC and DOE created this companion implementation guidance to assist entities wishing to adopt the Cybersecurity Baselines as the foundation of a cybersecurity risk management program. These entities may be electric distribution system and/or DER asset owners, and operators, and aggregators; state public utility commissions (PUCs) and other oversight bodies; state energy offices; or state legislators. A steering group consisting of state utility regulators, distribution system and DER owners and operators, trade organizations, and energy cybersecurity experts from across the sector and the country assisted in the development of this guidance.

The guidance in this document is interim, meaning that additional content will be added and refined in a final version. Until the final version is released, this interim guidance can inform key considerations and resource requirements and similar issues that entities should consider as they work to implement the Cybersecurity Baselines.

What's Included in the Interim Guidance: Scoping and Prioritizing the Cybersecurity Baselines

This Interim Implementation Guidance addresses two specific topics that can inform baseline implementation strategies: scoping and prioritization.

1. **Scoping:** considerations for the **scope of assets** to which the Cybersecurity Baselines should apply, at a minimum, based on risk to the distribution system.

2. **Prioritization:** an initial **priority set of baselines** that an asset owner or operator should meet first, if all baselines cannot be met at once, allowing states to design progressive implementation approaches.

Stakeholders should use a risk-driven approach to determine which assets may be subject to the baseline requirements, balancing the cost, time, and resource requirements of implementing cybersecurity controls with the risks to the grid.

The final Implementation Guidance will further address implementation strategies and adoption considerations for states that choose to implement Cybersecurity Baseline requirements.

How the Guidance Can Be Used

This document was created to assist distribution system asset owners and operators; PUCs and oversight bodies; state energy offices and legislators; and other stakeholders to implement the Cybersecurity Baselines in a timely, effective manner.

States can use this interim guidance to:

- Inform the adoption of the Cybersecurity Baselines as voluntary or mandatory requirements for the asset owners and operators they oversee.

- Identify whether new jurisdictional authorities or legislation are needed to effectively implement baselines within a state.

  Note that current jurisdictional models may limit the oversight authority of PUCs and other regulatory bodies over some assets within the suggested scope of these Cybersecurity Baselines. This interim guidance recommends a scope for the baselines that addresses the current risk environment, irrespective of current oversight models and authorities.

- Identify where incentives or technical assistance would enable timely adoption.

Owners and operators can use this interim guidance to:

- Identify the scope of applicable assets and the resources needed to implement the Cybersecurity Baselines.

- Prepare and execute plans to meet the baseline requirements.

Scope

Ideally, distribution system asset owners and their oversight bodies should use a risk-based approach to determine which assets are most critical to adopt the Cybersecurity Baselines. The challenge today, however, is that there is no widely accepted process for assessing risk and determining asset criticality that can be universally and consistently applied across the distribution system. The tables in subsequent sections provide examples of means, methods to, and ways of establishing consistent scope of asset that is informed by risk-based approaches.

The recommended scope is intended to help states establish a risk-informed definition of assets that can be consistently applied, offering multiple benefits. It allows owners and operators to concentrate their time and resources on mitigating risks to their most critical assets first. A clear definition that can be applied consistently across different asset owners is also useful to PUCs or other regulatory bodies interested in mandating Cybersecurity Baselines or offering material incentives for voluntary adoption. It also provides a roadmap for asset owners and operators that helps optimize their cybersecurity efforts and mitigate risks to their most critical assets first.

A clear definition typically includes a set of qualifiers, often called "bright lines" because they draw a clear distinction between assets that fall in scope or out of scope. These qualifiers are notoriously imperfect when applied industry wide, as risks vary based on system size, configuration, and load. However, they may help to define a consistent, risk-based scope in the absence of a common and consistent approach to risk assessment. Terms such as "all" or "any" have been intentionally excluded from the scope, allowing for conversations between asset owners and state regulators to address edge cases.

Elements of the Scope

The Cybersecurity Baselines were developed for distribution system assets below the bulk electric system (BES) designation.[4] The recommended scope contains two elements:

1. **The "Applicable Systems and Services"** scopes the baselines to those distribution system assets that are critical to providing reliable energy to customers (and particularly critical loads).
2. **The "Qualifiers"** further narrow the scope to the subset of assets deemed highest risk based on their potential impact to system. Each qualifier should be designed to determine in-scope assets consistently across all owners. Qualifiers should be considered as a multi-factor test, meaning that an asset only needs to meet one of the qualifiers to be considered in scope. Examples have been provided that implementers may choose in setting the qualifiers.

An asset is considered in scope if it is **an applicable system or service that also meets one or more of the qualifiers**. Organizations have the flexibility to and are encouraged to extend the application of baselines beyond the recommended scope, independent of mandatory requirements. Applying a single standard for cybersecurity controls to similar assets, systems, and networks is considered a best practice for cybersecurity hygiene.

The scope and qualifiers are presented separately for distribution system assets and DERs for ease of reference.

4. The bulk electric systems includes transmission assets operated or connected at 100 kV or higher. See: NERC, Glossary of Terms Used in NERC Reliability Standards, last updated January 7, 2025, *https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf.*

Scope of Distribution System Assets

Traditionally owned and operated by a distribution utility

Applicable Systems and Services

Defines the assets critical to providing reliable energy to customers that may be subject to the baselines

1. Systems or services that can be used to **directly change power flow or power quality** through digital means.
2. Systems, equipment, or services that are used by system operators to **remotely monitor power system conditions[5] and dispatch or control power system equipment**, whether from a centralized control center or from transient assets or tools.
3. **Microprocessor-based protective relays associated with power delivery equipment**, even where the relay's operation or failure to operate may not directly change power flow or power quality.
4. Systems, equipment, or services used for **automated data exchange**, where that data is **necessary for reliability and power security functions**, including where exchanged with BES entities.

Qualifiers for Applicability of Baselines

Used to further define the subset of assets that may be subject to the baselines based on highest risk

Qualifying Consideration to Determine Applicability	Example Qualifiers for each Consideration
Disruption to the system/service/network can impact energy delivery to a significant amount of distribution system load, considering one or more of the following: the total number of meters impacted, the MW of load impacted, or impacts to a percentage of the utility's total customer base or total distribution system load.	Impacts energy delivery to 50,000 customers[6] (or higher based on load density).
	Impacts 100 MW or more of distribution system load (for operators with less than 100MW of total distribution system load: impacts a risk-informed percentage of total distribution system load).
Disruption to the system/service/network can impact power delivery to a critical load, as determined by the PUC or system operator.	Critical loads may include: supply to facilities critical to national, state, or municipal security, including defense facilities (often defined by federal or state governments); facilities serving public health and safety; loads critical to system operation; etc.
A centralized management or control system[7] that operators use to monitor, dispatch, or control a significant amount of load.	An energy management system or distribution management system with external routable connectivity and ability to control more than 300 MW.

Important Note on Qualifiers

System sizes and densities vary dramatically by state and region, making it difficult to identify a single set of qualifiers that applies proportionately to all operators. For example, the provided example qualifier "Disruption to the system/service/network can impact energy delivery to 50,000 customers" would de- scope all assets for a small cooperative utility with only 30,000 customers, yet in-scope nearly every asset for a utility serving a large city with high load density. Regulators may want to use a qualifier such as percentage of impact to customers, especially for smaller utilities, considering the varying sizes of their customer bases.

5. Systems used solely to remotely monitor conditions may be in scope if those systems are used to inform control decisions.
6. The basis for this number includes the *DOE-417 Electric Emergency Incident and Disturbance Report*, which requires reporting of outages affecting 50,000 customers or more.
7. Such centralized management/control systems bring multiple assets to single points of access, which increases the potential impact/consequence of a cyber security event focused on that centralized system.

Scope of Distributed Energy Resources

Can be owned or operated by a variety of stakeholders, including traditional utilities, resource aggregators, and utility customers

Applicable Systems and Services

Defines the assets critical to providing reliable energy to customers that may be subject to the baselines

5 **Distributed energy resources (DER)**, defined as distribution-level generation, storage, and controllable load, and the communication systems and networks that support DERs.[8]

Qualifiers for Applicability of Baselines

Used to further define the subset of assets that may be subject to the baselines based on highest risk

Qualifying Consideration to Determine Applicability	Example Qualifiers for each Consideration
Individual or aggregated devices/systems/services[9] that, if if disrupted or intentionally misoperated, could result in a significant MW loss of load or supply of energy, or disrupt a significant percentage of local distribution system capacity.	An entity that has the ability to increase and/or decrease energy capacity and/or consumption of 100 MW or 10% of the local distribution system capacity (whichever is lower) from individual or aggregate resources.
Devices/systems/services that are digitally[10] connected to the distribution operator's system.	DERs permanently connected to the distribution grid with a direct digital connection, including behind-the-meter assets.

Recognizing Emerging DER Risks and Prioritizing Protection Strategies

DERs are typically small- to mid-scale modular systems that generate or store electricity, often near the point of consumption, or are systems of devices that enable controllable load. As DERs gain broader adoption, they offer an increasingly dynamic and decentralized way to produce and manage electricity, both locally and at scale.

The scope recommended in this interim guidance prioritizes DERs that represent significant capacity—whether individually or in aggregate—or those that have a direct digital connection to the distribution system operator. These can include community solar farms, virtual power plants, commercial DER systems, and aggregators of consumer-level DERs (such as bi-directional electric vehicle [EV] chargers and rooftop solar). Large DERs over 20 MW fall under federal oversight (under NERC CIP standards) and are therefore outside of scope.

PUCs and distribution system operators have a stake in mitigating cyber risks introduced by a high concentration of DERs connected to the local distribution system, even though such devices may not individually pose significant risk. When developing DER security strategies, regulators and system operators should consider these two key priorities:

1. Focus first on the most common DERs based on aggregated capacity: Prioritize applying the baselines to DERs that have the highest interconnected capacity in the service area.

2. Address DERs connected to the internet: Prioritize the security of DERs that are directly connected to the internet, as they are more exposed to potential cyber attacks.

8. This includes, but is not limited to, systems used to control the DERs as well as aggregate and dispatch resources.
9. Systems and services that are electrically connected to the distribution system, regardless of their digital connection.
10. Digital connection indicates a digital interaction between the resource and the utility, whether directly or through an aggregator.

DER Standards Can Simplify Baseline Adoption

To meet many of the baselines, asset owners and system operators should ensure the devices and systems that they own or connect to their systems are manufactured to meet the device-specific requirements outlined in the baselines (such as password management, encryption, and multi-factor authentication). There are several widely recognized Internet of Things (IoT) cybersecurity standards that provide a strong security foundation and align with baseline requirements.

DER devices and systems can be considered to meet the baselines if they meet one or more of the relevant DER standards outlined in the *Open EI DER Cyber Standards Library*[11] that can be mapped to the baselines. [Note: This effort published a *draft mapping* in February 2024 that aligned several informative references to the baselines. An updated mapping with validated alignment is expected in mid 2025.] Many of the standards include third-party certification processes that validate device performance to the standards.

Distribution system asset owners can use these standards in their procurement requirements and interconnection agreements, much like they do for fire and electric safety requirements. These standards help to ensure that consumer-grade IoT devices—such as EV chargers, heat pumps, smart thermostats, and photovoltaic (PV) inverters—incorporate cybersecurity best practices of the distribution systems operators. By adhering to these standards—or better yet, obtaining third-party certification of compliance—DER equipment manufacturers can demonstrate that their devices meet these requirements.

Recognizing Limitations on Jurisdictional Authority for DERs

As noted earlier, current regulatory models likely limit the oversight authority of PUCs and other regulatory bodies over DER assets, their owners/operators, or their manufacturers. The recommended scope addresses the current risk environment and is not limited by current oversight models.

11. Developed by the National Renewable Energy Laboratory (NREL) in coordination with the U.S. Department of Energy.

Prioritizing Baseline Implementation

Preferably, the entirety of the 35 Cybersecurity Baselines should be applied to assets that meet the scope outlined above. However, time and resource constraints may make an "all-at-once" approach impractical. PUCs and other oversight bodies may consider using a staged implementation of the baseline requirements, allowing organizations to reach full maturity over time.

This effort has identified **15 immediate priority baselines for distribution system asset owners and operators, and an additional 6 priority baselines for entities that own, integrate, or aggregate significant DER capacity.** See the *Cybersecurity Baselines for Electric Distribution Systems and DER* for the full text of the baselines referenced here.

The 15 immediate priorities represent those Cybersecurity Baselines that can most significantly reduce risk, while forming the basis for a more mature cybersecurity program. The six additional priorities for DER assets address the additional risks to the distribution system from integrating digital assets outside of the security perimeter of the distribution system operator. To simplify baseline adoption, asset owners can procure and interconnect DER systems that are manufactured to recognized industry standards, which align with the device-specific requirements outlined in the baselines (see the section *"DER Standards Can Simplify Baseline Adoption"*).

These priority baselines are deliberately unweighted so that the order of implementation within the prioritized list can be determined by each distribution system asset owner, based on their individual system design, maturity, and risk environment. Asset owners may wish to implement these in tandem with other Cybersecurity Baselines not on this initial priority list for cost efficiency.

Priority Baselines for All In-Scope Assets

1.A – Asset Inventory

1.B – Organizational Cybersecurity Leadership

1.C – OT Cybersecurity Leadership

1.D – Improving IT and OT Cybersecurity Relationships

1.E – Mitigating Known Vulnerabilities

2.A – Changing Default Passwords

2.B – Password Management

2.D – Revoking Credentials for Departing Employees

2.E – Separating User and Privileged Accounts

2.F – Network Segmentation

2.H – Phishing-Resistant Multifactor Authentication (MFA)

2.I – Basic Cybersecurity Training

2.P – Document & Maintain Network Topology

2.R – System Backups

2.W – No Exploitable Services on the Internet

2.X – Limit OT Connections to Public Internet

5.A – Incident Planning and Preparedness

Additional Priority Baselines for In-Scope DER Assets

1.F – Third-Party Validation of Cybersecurity Control Effectiveness

1.I – Vendor/Supplier Cybersecurity Requirements

2.T – Log Collection

2.U – Secure Log Storage

2.V – Prohibit Connection of Unauthorized Devices

4.A – Incident Reporting

See the *Cybersecurity Baselines for Electric Distribution Systems and DER* for the full text of the baselines referenced here.

What's Next?

This interim guidance focuses on two topics essential to Cybersecurity Baselines implementation: asset scoping and baseline prioritization. This information helps focus implementation to the most critical assets and protects them via application of the highest-priority baselines. The intention is to provide a starting point from which a solid cybersecurity foundation can be built and later expanded upon, following a risk-informed roadmap.

The next step is to develop more detailed implementation guidance for entities interested in adopting the Cybersecurity Baselines as foundational cybersecurity requirements. Guidance will consider both voluntary and mandatory settings and include considerations for stakeholders of differing ownership models, sizes, and maturity levels. Topics such as engagement strategies, compliance approaches, and resource requirements will be included.

When completed, a final guidance will replace this interim draft. Look for the final version of the Implementation Guidance for Cybersecurity Baselines for Distribution Systems and DERs in mid-2025.

Visit the Cybersecurity Baselines website for more information: *https://www.naruc.org/core-sectors/critical-infrastructure-and-cybersecurity/cybersecurity-for-utility-regulators/cybersecurity-baselines/*

www.naruc.org