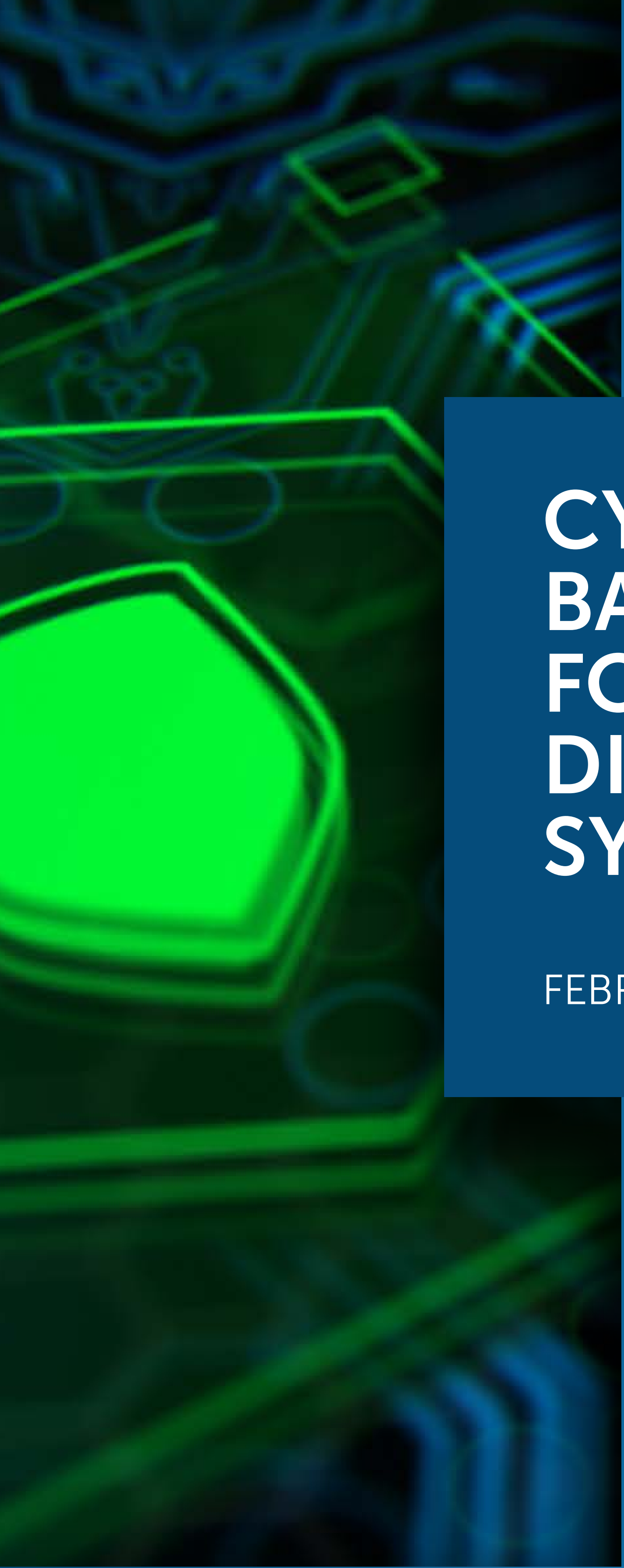

CYBERSECURITY BASELINES FOR ELECTRIC DISTRIBUTION SYSTEMS AND DER

FEBRUARY 2024

U.S. DEPARTMENT OF ENERGY

NARUC
National Association of Regulatory Utility Commissioners

TABLE OF CONTENTS

Executive Summary

The National Association of Regulatory Utility Commissioners (NARUC) has partnered with the Department of Energy (DOE) to develop a set of cybersecurity baselines for electric distribution systems and the distributed energy resources (DERs) that connect to them. Cybersecurity is an integral underpinning of power system resilience, and this initiative builds on work that states have undertaken over the last decade to mitigate cybersecurity risk across their critical infrastructures.

Electric distribution system stakeholders recognize the importance of enhancing grid reliability, resilience, and security. Indeed, addressing cybersecurity risk is essential as electric distribution systems continue to evolve, spurred by new technologies and operational models as well as the ever-increasing threat of cyber-attacks. The National Cybersecurity Strategy, issued in 2023, also directed the U.S. Department of Energy (DOE) to "promote cybersecurity for electric distribution and distributed energy resources (DERs) in partnership with industry, states, federal regulators, Congress, and other agencies." This NARUC/DOE initiative complements industry and government efforts by providing cybersecurity baselines, tailored for electric distribution systems and the DERs that connect to them, creating a common starting point for cyber risk reduction activities.

These baselines, coupled with the forthcoming implementation guidance, are intended to be a resource for state Public Utility Commissions, electric distribution utilities, and DER operators and aggregators. They encourage alignment across states that choose to adopt the baselines to mitigate cybersecurity risk and enhance grid security. NARUC convened a Steering Group of regulatory, cyber, and industry experts from across the sector to help execute this challenging task. The development process also included multiple stakeholder review and comment cycles to ensure a wide range of perspectives were considered.

This initiative is divided into two phases:

- **Phase 1:** Development of a vetted set of **Cybersecurity Baselines** for Electric Distribution systems and the DERs that connect to them. These baselines define the cybersecurity controls that should be implemented, without specifying which procedures or technologies to use. It is expected that the baselines may be used by regulatory bodies and distribution utilities as a potential framework for developing their own cybersecurity requirements in conjunction with Phase 2 implementation strategies.
- **Phase 2:** Preparation of **Implementation Strategies and Adoption Guidelines** to support electric distribution system stakeholders as they continue to develop and refine their cybersecurity requirements. These Implementation Guidelines will include recommendations for assessing cybersecurity risks, prioritizing the assets to which the cybersecurity baselines might apply, and prioritizing the order in which the baselines might be implemented based on cyber risk assessments. The guidance will also address risk-based implementation timelines. The Implementation Strategies and Adoption Guidelines are aimed at Public Utility Commissions, utilities, and DER operators who wish to adopt the baselines. Phase 2 is expected to be completed over the course of the next year.

The Phase 1 Cybersecurity Baselines are intended to be used in concert with Phase 2 Implementation Guidance. Implementing the baselines without thoughtful consideration of scope, priorities, sequencing, and risk may result in the inefficient use of limited resources on the part of Commissions, distribution utilities, and DER providers and aggregators, thus diluting the effectiveness of cyber protections being applied where they matter most. Publishing the baselines now while undertaking Phase 2 allows for broader awareness of their development and provides an opportunity for commissions to engage in discussions with key stakeholders within their jurisdictions as the implementation guidance is being designed.

Phase 2 will tailor cybersecurity controls that focus on addressing risk to the different stakeholders that participate in the distribution system. The number of distribution system participants continues to increase, and each participant faces different types of risk based on entity sizes, architectures, components, and control mechanisms of power systems. Those risks will evolve over time as the power systems change, and as technologies advance and become more pervasive. Phase 2 will develop implementation guidelines based on these and other factors. As Phase 2 develops, enhancements to the baselines may be suggested.

Development of Cybersecurity Baselines

Rather than starting from scratch, NARUC,DOE, and the Steering Group recognized the importance of leveraging existing resources when developing these baselines. The Department of Homeland Security Cybersecurity and Infrastructure Security Agency's (DHS/CISA) Cybersecurity Performance Goals (CPGs) were selected as the starting point because they are risk-informed, and intended to be tailored to each particular industry's use. The CPGs were created to inform protections that could be deployed by sectors that had not already adopted more sophisticated and robust security practices. Work done during Phase 1 tailors the CPGs for electric distribution systems and the DERs that connect to them. Tailoring of the CPGs took into consideration existing cybersecurity frameworks, standards, and best practices, especially those within the electric sector. A key focus for the steering group was to promote risk-informed cybersecurity practices that, when applied, produce demonstrable cybersecurity benefits. Phase 2 will continue this risk informed focus and provide guidance, designed to help states and others interested in effectively implementing the baselines to achieve risk-informed, cost-effective cybersecurity objectives across their electric distribution systems.

Cybersecurity Baselines for Electric Distribution Systems and DER

1.A Asset Inventory

Maintain an inventory of critical IT and digital OT assets, using the organization's risk-based criteria for classifying the criticality of assets that are essential to the delivery of energy.

1.B Organizational Cybersecurity Leadership

1.C OT Cybersecurity Leadership

1.D Improving IT and OT Cybersecurity Relationships

Designate a senior-level role/title/position with explicit accountability for governance, planning, resourcing, and executing IT and OT cybersecurity activities. Identify the senior-level role(s)/title(s)/position(s) with delegated responsibility for planning, allocating resources, managing, and executing cybersecurity activities while promoting a culture of cybersecurity.

1.E Mitigating Known Vulnerabilities

Establish and implement a vulnerability management plan to address known exploited vulnerabilities, prioritizing critical assets identified in 1.A. Identify compensating controls for critical assets where removing the vulnerability is either not possible or may substantially compromise availability or safety.

1.F Third-Party Validation of Cybersecurity Control Effectiveness

Develop and implement a plan for periodic independent validation of the organization’s cybersecurity controls and mitigate findings in a timely, risk-informed manner.

1.G Supply Chain Incident Reporting

1.H Supply Chain Vulnerability Disclosure

As new procurements are made for critical devices or services, make a good-faith effort to negotiate procurement documents and contracts stipulating that vendors and/or service providers:

Notify the procuring customer of security incidents within a risk-informed time frame, as determined by the organization.

Notify the procuring customer of confirmed security vulnerabilities in their assets within a risk-informed time frame, as determined by the organization

1.I Vendor/ Supplier Cybersecurity Requirements

Include cybersecurity requirements and questions, as appropriate, in the organization’s procurement process, and evaluate responses as part of the vendor selection.

2.A Changing Default Passwords

Establish and maintain a process to change default passwords before installation. Document and implement equally or more effective alternative methods or compensating controls where exceptions are necessary.

2.B Password Management

Establish and enforce a policy that requires a minimum password length of 15 or more characters for in-scope IT and OT assets that are not otherwise protected behind multi-factor authentication (MFA) or other passwordless authentication mechanism.

- If 15-character passwords, MFA, or other passwordless authentication mechanisms are not feasible, use the maximum password length that the technology supports and document and implement equally or more effective alternative measures or compensating controls to achieve the intended action(s).

Establish and enforce a policy to prohibit password reuse, unless an organization-defined risk exception is necessary and documented.

2.C Unique Credentials

Provide unique and separate credentials for users accessing services and assets on IT and OT networks. Establish and implement a process to manage and approve access to shared accounts / service accounts / machine accounts. Document and implement equally or more effective alternative methods or compensating controls where exceptions are necessary.

2.D Revoking Credentials for Departing Employees

Establish and enforce an administrative process to (1) revoke physical access and (2) disable logical access to critical organizational resources within 24 hours of an employee's separation unless an organization-defined risk exception is necessary and documented.

2.E Separating User and Privileged Accounts

Establish and maintain a policy to restrict administrator rights on user accounts on critical assets. Require separate user accounts for actions and activities not associated with the administrator role (e.g., for business email, web browsing). Reevaluate privileges on a recurring basis to validate continued need for a given set of permissions.

Document and implement alternative measures or compensating controls in instances where administrative privileges cannot be removed.

2.F Network Segmentation

Separate IT and OT networks, and OT networks of different trust levels.

- Use an appropriate network security device to enforce a deny-by-default policy on communications between networks that permits only those connections that are explicitly allowed (e.g., by IP address and port) for specific system functionality.
- Maintain documentation of allowed ports and services and their business justification.

2.G Unsuccessful (Automated) Login Attempts

Implement a process to detect, alert, and monitor unsuccessful logins and to inform the appropriate personnel. Document and implement equally or more effective alternative methods or compensating controls where exceptions are necessary.

2.H Phishing-Resistant Multifactor Authentication (MFA)

Implement MFA for remote access to assets using the strongest available method for that asset and where technically feasible. Document and implement equally or more effective alternative methods or compensating controls where exceptions are necessary.

2.I Basic Cybersecurity Training

Conduct training, at least annually, for all organizational employees and contractors that cover basic security concepts, such as phishing, business email compromise, basic operational security, password security, etc., as well as foster an internal culture of security and cyber awareness.

- New employees receive initial cybersecurity training within 30 days of onboarding and recurring training on at least an annual basis.
- Training topics and goals are clearly defined and related to the nature of their duties to the extent practicable.

2.J OT Cybersecurity Training

In addition to basic cybersecurity training, conduct OT-specific cybersecurity training, at least annually, for personnel who access or secure OT as part of their regular duties.

2.K Strong and Agile Encryption

Establish and implement a policy that addresses the protection of critical data in transit, including how the organization will update outdated/deprecated encryption technologies or document and implement equally or more effective alternative methods or compensating controls.

2.L Secure Sensitive Data

Establish and maintain a process to identify and securely store sensitive data, using strong access control methods for authenticated and authorized users and system applications. Document and implement equally or more effective alternative methods or compensating controls where exceptions are necessary.

2.M Email Security

Establish and maintain a process to reduce risk from email threats.

2.N Disable Macros by Default

Establish software restriction policies to prevent the execution of unauthorized code, such as a system-enforced policy that disables Microsoft Office macros, or similar embedded code, by default. If macros must be enabled in specific circumstances, establish a policy for authorized users to request that macros are enabled on specific assets, for only as long as they are needed. Document and implement equally or more effective alternative methods or compensating controls where exceptions are necessary.

2.O Document Device Configurations

Document, backup and maintain baselines and current configuration details of critical IT and OT assets to facilitate more effective vulnerability management and response and recovery activities. Periodically review and update documentation.

2.P Document & Maintain Network Topology

Document, backup and maintain physical and logical network topology across critical IT and OT networks. Review and document any change to the topology.

2.Q Hardware and Software Approval Process

Implement an administrative policy or automated process for critical IT and OT assets that requires approval before new hardware, firmware, or software/software version is installed or deployed, or before the asset is removed/decommissioned. Documentand implement equally or more effective alternative methods or compensating controls where exceptions are necessary.

2.R System Backups

Establish and maintain a documented system restoration plan, including processes to back up critical systems where deemed appropriate by the organization.

2.S Incident Response (IR) Plans

Establish, maintain, and regularly (at least annually) validate IT and OT cybersecurity incident response plans for both common and organizationally specific threat scenarios and TTPs through cybersecurity exercises.

- Update incident response plans within a risk-informed time frame to incorporate lessons learned from the exercise.

2.T Log Collection

Collect and develop a process to securely store and protect time-synchronized access- and security-focused logs (e.g., authentication, intrusion detection systems/intrusion prevention systems, firewall, data loss prevention, virtual private network) based on criticality for use in both detection and incident response activities (e.g., forensics).

- OT: For OT assets where logs are non-standard or not available, collect network traffic and communications between those assets and other assets where feasible.

2.U Secure Log Storage

Establish and maintain a process to protect logs for critical IT and OT assets from unauthorized access.

2.V Prohibit Connection of Unauthorized Devices

Establish and maintain policies and processes to reduce the probability that unauthorized media or hardware are connected to IT and OT assets, such as by limiting use of USB devices and removable media and disabling AutoRun.

- Define acceptable types of media and hardware and establish scanning requirements when appropriate for devices that have a storage component.
- Establish validation and authorization steps when new devices are connected to ensure no unauthorized devices are connected.
- OT: When feasible, establish procedures to remove, disable, or otherwise secure physical ports to prevent the connection of unauthorized devices or establish procedures for granting access through approved exceptions.
- Document and implement equally or more effective alternative methods or compensating controls where exceptions are necessary.

2.W No Exploitable Services on the Internet

Implement a process to minimize the number of ports and services exposed to the Internet.

- Prevent assets on the public internet from exposing services with known exploits.
- Where these services must be exposed, document and implement appropriate compensating controls to prevent common forms of abuse and exploitation.
- Disable unnecessary applications and network protocols on internet-facing assets.

2.X Limit OT Connections to Public Internet

Establish and implement a process to ensure OT assets are not placed on the public internet, unless explicitly required for operation. Document necessary exceptions and implement compensating controls for excepted assets to prevent and detect exploitation attempts (such as logging, MFA, mandatory access via proxy or other intermediary, etc.).

3.A Detecting Relevant Threats and TTPs

Maintain situational awareness of threats and cyber actor tactics, techniques, and procedures (TTPs) relevant to their organization (e.g., based on industry, sectors), and maintain the ability to detect instances of those key threats (such as via rules, alerting, or commercial prevention and detection systems).

4.A Incident Reporting

Establish and maintain codified policy and procedures on when, to whom, and how to report all confirmed cybersecurity incidents to appropriate external entities.

4.B Vulnerability Disclosure/Reporting

Establish and maintain a public, easily discoverable method for security researchers to notify the organization of vulnerable, misconfigured, or otherwise exploitable assets (e.g., via email address or web form). Acknowledge and respond to valid submissions in a timely manner, taking into account the completeness and complexity of the vulnerability. Mitigate validated and exploitable weaknesses consistent with their severity and organizational policy. Establish policies concerning coordinated vulnerability disclosure/reporting.

4.C Deploy Security.TXT Files

Ensure that public-facing web domains have a security.txt file that conforms to the recommendations in RFC 9116 “A File Format to Aid in Security Vulnerability Disclosure.”

5.A Incident Planning and Preparedness

Develop, maintain, and execute plans to recover and restore to service business or mission-critical assets or systems that might be impacted by a cybersecurity incident.

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*.

www.naruc.org

DISCLAIMER

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

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

U.S. DEPARTMENT OF ENERGY

NARUC
National Association of Regulatory Utility Commissioners