

Final

Security Guideline

Inverter-Based Resources

September 9, 2026

Table of Contents

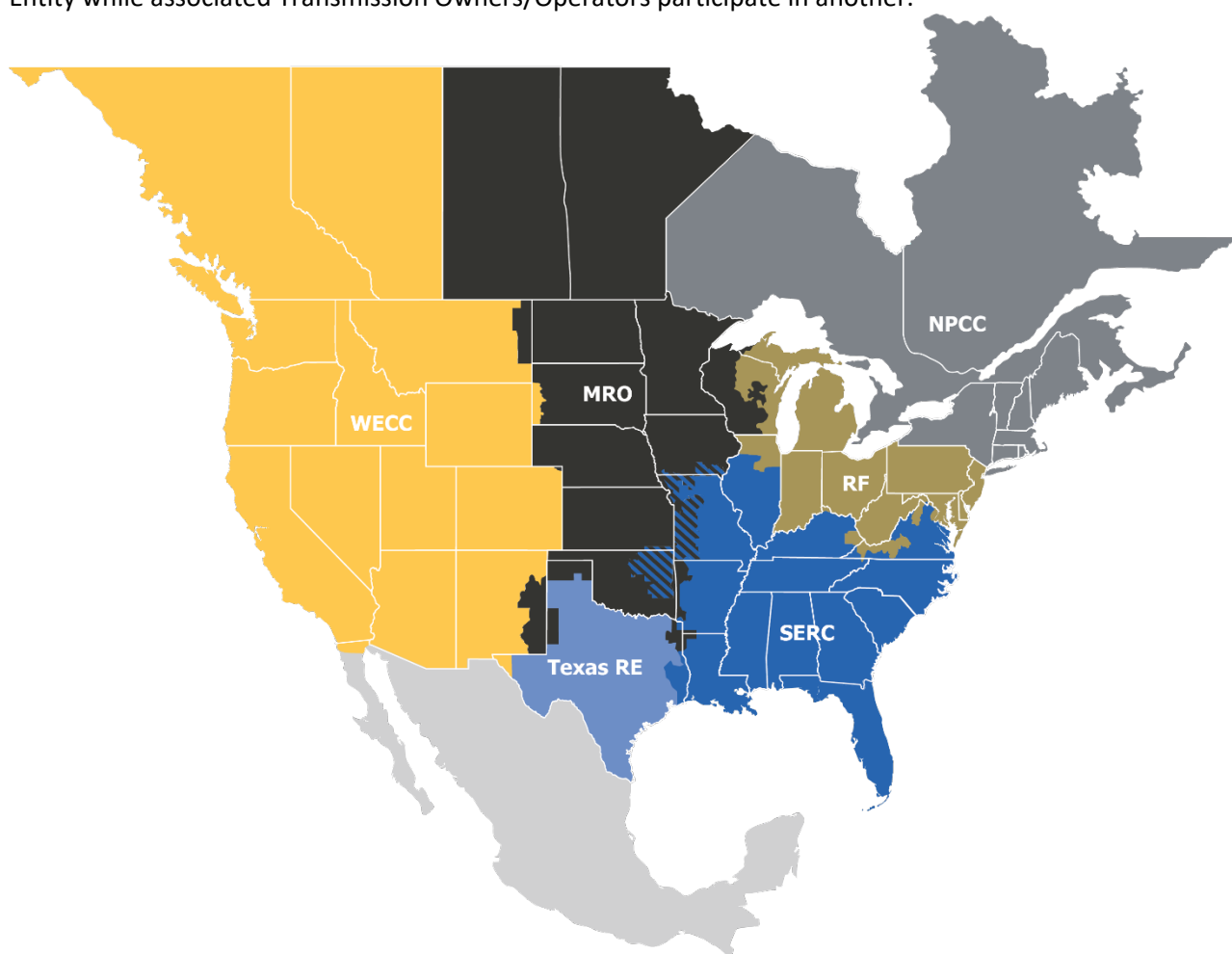
Preface	iii
Preamble.....	iv
Executive Summary	v
Chapter 1: Introduction and Scope.....	1
Target Audience	1
Security Objectives.....	1
Chapter 2: Supply Chain and Third-Party Dependency Management.....	3
Hardware and Software Procurement Controls	4
Vendor Security Posture and Contractual Expectations	5
Cloud and Third-Party Services	6
Ongoing Vendor and Third-Party Risk Management	7
Geographic and Jurisdictional Sourcing Considerations	7
Chapter 3: Identity and Access Management	9
Chapter 4: Remote Access and Network Connectivity	10
Chapter 5: Network Architecture and Segmentation	12
Baseline Practices:	12
Enhanced Practices:.....	13
Advanced Practices:	13
Internal Network Security Monitoring.....	13
Chapter 6: Asset Management and Configuration Control	15
Chapter 7: Information Classification and Protection	17
Chapter 8: Secure Communication Protocols and Telemetry	18
Chapter 9: Incident Response and Recovery Preparedness	20
Baseline Incident Response and Recovery Practices.....	20
Enhanced Incident Response and Recovery Practices	21
Chapter 10: Conclusion.....	23
Appendix A: Contributors	24
Appendix B: Guideline Information and Revision History	26
Appendix C: Metrics.....	27

Preface

Electricity powers our modern life and is the bedrock of our economic wellbeing. The Electric Reliability Organization (ERO) Enterprise—comprised of NERC and the six Regional Entities—is firmly committed to assuring a highly reliable, resilient, and secure bulk power system (BPS) in North America. The ERO Enterprise enables collaborative engagement with industry, regulators, and stakeholders, embracing innovation and supporting the needs of nearly 400 million people.

RELIABILITY | RESILIENCE | SECURITY **POWERING TODAY. PROTECTING TOMORROW.**

The North American BPS is made up of six Regional Entities as shown on the map and in the corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Regional Entity while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Preamble

The NERC Reliability and Security Technical Committee (RSTC), through its subcommittees and working groups, develops and triennially reviews reliability guidelines in accordance with the procedures set forth in the RSTC Charter. Reliability guidelines include the collective experience, expertise, and judgment of the industry on matters that impact BPS operations, planning, and security. Reliability guidelines provide key practices, guidance, and information on specific issues critical to promote and maintain a highly reliable and secure BPS.

Each entity registered in the NERC compliance registry is responsible and accountable for maintaining reliability and compliance with applicable mandatory Reliability Standards. Reliability guidelines are not binding norms or parameters nor are they Reliability Standards; however, NERC encourages entities to review, validate, adjust, and/or develop a program with the practices set forth in this guideline. Entities should review this guideline in detail and in conjunction with evaluations of their internal processes and procedures; these reviews could highlight that appropriate changes are needed, and these changes should be done with consideration of system design, configuration, and business practices.

Executive Summary

Utility-scale inverter-based resources (IBR), including solar photovoltaic generation, wind generation, and battery energy storage systems, are increasingly integral to BPS reliability. These resources rely on digital control and telemetry pathways that connect plant controllers, inverters, protection and automation functions, and off-site monitoring and dispatch capabilities. Compromise of these pathways can result in unauthorized control actions, loss of operational visibility, and loss of generating capability. There is broad variability in the maturity and consistency of cyber security implementation throughout the IBR build and integration lifecycle, ranging from misalignment between project delivery and security teams to the absence of security-by-design considerations. As IBR penetration increases, coordinated loss or manipulation across multiple facilities can create reliability risk that exceeds the impact of a single-site event.

This security guideline provides recommended practices intended to strengthen cyber security outcomes for utility-scale IBR facilities and supporting communications. The guideline is advisory and is intended to support the application of a practical baseline of cyber security controls that aligns with reliable operations across diverse IBR architectures, remote connectivity models, and third-party dependencies. The guidance is intended to be applied with consideration for site-specific architecture, operational requirements, and technical limitations of deployed hardware and software, including phased adoption where changes can affect system performance or availability.

The recommended practices in this guideline are organized to support the following objectives for IBR operations: preserve the confidentiality and integrity of IBR commands and telemetry; maintain availability of IBR generating capability by limiting attack paths that could disrupt operations, damage equipment, or impair operational visibility; and reduce the likelihood and impact of compromise through baseline expectations for identity and access management, asset management and configuration control, and secure communications and telemetry.

Key recommended practice areas addressed in this guideline include the following:

- Supply chain and third-party dependency management, including procurement expectations, contractual controls, and ongoing oversight of vendor access and updates
- Identity and access management, including unique identities, strong authentication, least privilege, and monitoring of access activity
- Remote access and network connectivity governance, including secure-by-default remote access, differentiated handling of interactive and machine-to-machine communications, and explicit control of vendor remote access
- Network architecture and segmentation practices, including baseline and advanced segmentation approaches and the use of operational technology (OT)-designed internal network security monitoring to improve visibility without disrupting operations
- Asset management and configuration control, including asset inventory, baseline configurations, patching and update processes, and backup and restoration readiness
- Secure communication protocols and telemetry practices, including protection of operational data in transit and management of embedded communications modules

Chapter 1: Introduction and Scope

This guidance focuses on utility-owned or -operated, grid-connected IBR facilities, including plants typically interconnected at sub-transmission or transmission voltage levels and utility-controlled, distribution-connected distributed energy resources (DER), such as microgrids. Smaller DER installations, including residential IBRs such as rooftop solar, are out of scope for this guideline. Many IBR facilities, including newly registered Category 2 IBRs, are not individually classified as Bulk Electric System (BES) facilities and are therefore not subject to existing NERC Critical Infrastructure Protection (CIP) requirements as of Q1 2026.

This security guideline, developed under SITES within NERC's RSTC, provides recommended practices intended to strengthen cyber security outcomes for utility-scale IBR facilities and supporting communications. The guideline is advisory and is intended to support the application of a practical baseline of cyber security controls that aligns with reliable operations across diverse IBR architectures, remote connectivity models, and third-party dependencies.

This guideline is intended to be applied with consideration for site-specific architectures, operational requirements, and technical limitations of deployed hardware and software. Implementation of recommended practices may require engineering review, testing, or phased adoption, particularly for existing IBR facilities where changes can affect system performance or availability. Entities should apply this guidance using sound engineering judgment, integrating cyber security considerations in a manner that supports reliable operations while addressing practical constraints.

Target Audience

This guideline is intended for the following stakeholders with responsibility for the implementation and operation of cyber security controls in utility-scale IBR environments:

- **Electric Utilities:** Transmission and distribution utilities integrating significant IBR capacity, including utilities that own or operate IBR facilities, DERs, or utility-controlled microgrids. This audience includes operational technology and industrial control system security personnel supporting these environments.
- **Category 1 and Category 2 Generator Owners and Generator Operators (GO/GOP):** Entities that own or operate utility-scale IBR facilities interconnected to the BPS, including independent power producers operating large solar, wind, or battery energy storage plants.
- **Original Equipment Manufacturers (OEM) and Integrators:** Manufacturers of IBR equipment and engineering, procurement, and construction (EPC) organizations involved in the design, integration, and commissioning of IBR facilities. While not the primary audience for this guideline, these stakeholders play a significant role in enabling secure configurations, access controls, and lifecycle support for deployed systems.

Security Objectives

While cyber security risk exists across all IBR assets, it is not practical to apply uniform security controls across all facilities and configurations. IBR assets that fall below the applicability thresholds of current mandatory requirements are often deprioritized for cyber security, resulting in little or no applied security treatment. Entities responsible for IBR assets addressed by this guideline should evaluate those assets against a minimum baseline of applicable cyber security practices, such as those described in this guideline or those required for low-impact BES cyber systems under CIP-003 Requirement R2.

The recommended practices in this guideline are organized to support the following objectives for IBR operations:

- Preserve the confidentiality and integrity of IBR commands and telemetry to reduce the likelihood of unauthorized control or data manipulation
- Maintain availability of IBR generating capability by limiting attack paths that could disrupt operations, damage equipment, or impair operational visibility
- Reduce the likelihood and impact of compromise by establishing baseline expectations for identity and access management, asset management and configuration control, and secure communications and telemetry

Although this guideline focuses on cyber security, physical access to IBR facilities remains an important contributor to overall risk. Many IBR sites are remotely located, minimally staffed, or unattended, which can increase exposure to unauthorized access or tampering. Physical access to communications equipment, control devices, or networking infrastructure can bypass or weaken cyber protections and should be considered as part of the broader security context.

Expectations for physical security vary significantly based on site characteristics, operational impact, and realistic threat conditions. Physical security measures are typically applied on a risk- and site-specific basis, balancing cost, practicality, and potential impact. While IBR facilities are not generally designed to be hardened against all physical threats, even basic deterrence and tamper awareness can reduce the likelihood of undetected interference and support timely response.

Detailed physical security design and threat modeling are outside the scope of this guideline. However, entities are encouraged to consider physical and cyber risks together and to align physical protection expectations with the role of the IBR facility in supporting reliable operations. Additional risk-based physical security practices are provided in NERC's *Voluntary Physical Security Protection Best Practices at Entity Facilities* (March 2026).¹

¹ https://www.nerc.com/globalassets/our-work/guidelines/security/sg_voluntary_physical_security_protection_best_practices_at_entity_facilities.pdf

Chapter 2: Supply Chain and Third-Party Dependency Management

Utility-scale IBR facilities rely on a layered vendor ecosystem that extends beyond primary equipment manufacturers. Typical deployments include inverter and plant controller platforms, site networking and telecommunications services, remote monitoring and support tooling, and software and firmware dependencies, managed compliance and managed security service providers that persist throughout the asset lifecycle. These relationships and dependencies are operationally necessary, but they also expand the set of trusted components, trusted parties, and trusted pathways that can affect IBR performance and availability. These dependencies increasingly include cloud-hosted services and potentially artificial intelligence (AI)-enabled analytics or support capabilities.² Entities should identify how such technologies are used, which parties operate them, what data or control functions they affect, and how compromise or loss of service could propagate through layered suppliers.

Supply chain and third-party risk in IBR environments are shaped by several characteristics that are common across modern deployments: software-defined behavior, frequent firmware or configuration updates to maintain performance and compliance, and routine remote access for commissioning, tuning, diagnostics, maintenance, and warranty claims. These practices increase exposure to risks introduced through compromised updates, insecure vendor tooling, or mismanaged third-party access. In addition, repeated designs and common vendor stacks across multiple sites can create fleet-wide exposure when a single dependency is compromised.

Supply chain and third-party cyber security expectations are often constrained by existing contractual arrangements and vendor relationships, particularly for deployed IBR facilities. While entities may have limited ability to impose new requirements mid-term, this does not eliminate the need to define and apply clear security expectations for third-party access, services, and dependencies. Entities should treat vendor and contractor cyber security requirements as enforceable policy objectives, applied on a risk-informed and per-contract basis and incorporated where feasible through contract renewals, amendments, technical standards, and operational procedures. Over time, consistent application of these expectations across vendors and contract cycles reduces unmanaged risk, even where immediate uniform adoption is not practical. Entities should integrate these expectations into existing cyber security, procurement, vendor risk management, and change control programs rather than establish isolated IBR-specific processes where mature controls already exist.

Entities should consider that usage of any engaged managed compliance service providers (MCSP) and managed security service providers (MSSP) for the delegation of the security posture of their IBR assets and networks necessitates continued oversight from the entity rather than hands-off treatment with the MCSP or MSSP. A “trust but verify” practice should be used, maintaining an ongoing conversation with such entities regarding up-to-date knowledge and security practices such as those provided herein.

This chapter addresses supply chain and third-party dependency risk as a direct reliability consideration for IBR operations. It focuses on the risks introduced through equipment and software provenance, update and support channels, and persistent external access pathways into IBR asset networks. For purposes of this guideline, critical IBR components are those that enable or support control, protection, communications,

² For additional cloud risk and mitigation considerations, see NERC, BES Operations in the Cloud (September 2023), https://www.nerc.com/globalassets/our-work/white-papers/sites/whitepaper_bes_ops_in_cloud.pdf; and NERC Project 2023-09, Risk Management for Third-Party Cloud Services, <https://www.nerc.com/standards/reliability-standards-under-development/2023-09-risk-management-for-third-party-cloud-services>

monitoring, or external connectivity, such as inverters, power conversion systems, plant controllers, gateways, communications platforms, and supporting cloud services.

Hardware and Software Procurement Controls

Cyber security risk in IBR environments is often introduced during design and procurement. Hardware and software selected without defined security expectations can create long-term operational constraints and persistent attack paths. The following recommended practices address cyber security considerations that should be incorporated into procurement of IBR-related hardware and software:

- **Incorporate cyber security requirements into procurement specifications.** Cyber security expectations should be defined in requests for proposal (RFP), procurement specifications, and acceptance criteria alongside functional and performance requirements. These expectations should apply, as appropriate, to IBR hardware, software, programmable devices, services, delivered configurations, and supporting components. For products that perform or support critical IBR functions, procurement specifications should require software bills of materials (SBOM) and, where practicable, hardware bills of materials (HBOM); contracts should define update frequency, handling of sensitive BOM information, and rights to validate delivered components against approved BOMs or equivalent evidence. Entities should communicate these requirements to OEMs, EPC contractors, and integrators early enough to influence design, component selection, testing, commissioning, and system acceptance. Procurement decisions should account for the ability of the product or vendor to support secure configuration, access control, update mechanisms, and vulnerability response throughout the asset lifecycle.
- **Evaluate vendor security posture as part of product selection.** Entities should consider a vendor's security practices, development processes, and history of vulnerability management when selecting equipment or software for IBR environments. Products that cannot reasonably support secure operation, maintenance, or updates should be avoided where alternatives exist.
- **Account for supply chain risk in vendor and product selection.** Procurement processes should consider risks associated with vendor origin, manufacturing, software development, and support models. Where appropriate, entities should consult publicly available lists of high-risk products and entities (e.g., the Federal Communications Commission's supply chain covered list and the U.S. Department of Commerce Entity List) and incorporate screening against denied or restricted party lists into procurement and approval processes. The assessment should consider how the vendor, delivered product, or supporting service could transfer cyber security and operational risk to the entity at delivery and throughout the support lifecycle.
- **Establish acceptance criteria for software and firmware integrity.** Software and firmware used in IBR environments should support mechanisms to verify authenticity and integrity prior to installation or execution. Procurement specifications should require that update mechanisms protect against unauthorized or modified code being introduced into operational systems.
- **Require transparency and notification for product vulnerabilities.** Vendors should be expected to notify asset owners of identified security vulnerabilities affecting deployed products and to provide guidance or updates to address those vulnerabilities within a reasonable time frame. Procurement expectations should clarify how vulnerability information is communicated and how updates are made available. Vendors should also disclose material cloud services, embedded third-party software, and other supplier dependencies that could affect security, availability, or vulnerability response.

Vendor Security Posture and Contractual Expectations

IBR owners and operators should address cyber security risk associated with vendors, integrators, and service providers through defined security expectations and enforceable contractual terms. Vendor security posture and access conditions directly affect the security of IBR operational environments and should be evaluated and managed throughout the vendor relationship, not only at initial procurement. The following practices are recommended for managing vendor security and contracts:

- **Evaluate vendor cyber security posture prior to engagement and periodically thereafter.** Entities should assess whether vendors supporting IBR environments maintain security practices appropriate to the level of access and dependency involved. The depth of evaluation should be commensurate with risk and may include questionnaires, attestations, or independent assessments where appropriate.
- **Require secure configuration and hardened defaults for delivered systems.** Vendors and integrators should deliver hardware and software in a secure configuration, with unnecessary services disabled, default credentials removed, and access controls aligned to the owner's security expectations. Secure configuration requirements and all existing (e.g., pre-configured) remote, vendor, and administrative access paths should be reviewed, verified, and aligned with the entity's security requirements before system acceptance and integration.
- **Define and enforce conditions for vendor remote access.** Vendor remote access should be permitted only through owner-approved access mechanisms and under defined conditions. Contracts should prohibit unmanaged or persistent access paths and require strong authentication, encryption, logging, and owner authorization for remote access activities. Vendor access requirements and implementation should align with the entity's existing identity, access management, and remote access controls whenever possible.
- **Establish expectations for vulnerability disclosure and patch support.** Vendors should be contractually obligated to notify asset owners of security vulnerabilities affecting delivered products and to provide patches or mitigations within reasonable time frames. Expectations for patch availability and vendor support should reflect the operational role of the affected systems.
- **Require incident notification and cooperation.** Vendors should be required to promptly notify asset owners of security incidents that could affect IBR systems or supporting services. Contracts should preserve the owner's ability to suspend or terminate vendor access in response to security concerns.
- **Apply vendor security expectations consistently over time.** Where immediate enforcement is not feasible due to existing agreements, entities should incorporate these expectations into contract renewals, amendments, and future engagements to reduce unmanaged third-party risk over the lifecycle of IBR assets. Applicable security expectations from this guideline, including identity and access management, remote access, configuration and change management, secure communications, incident notification, evidence preservation, and response participation, should be reflected in procurement specifications, contracts, and service agreements, as appropriate.
- **Apply project-specific findings and lessons learned across the IBR portfolio.** Entities should evaluate whether vulnerabilities, control improvements, or network upgrades identified during a project apply to other IBR assets under the same ownership and should track resulting actions to completion. Vendor requirements and related control documentation should also be reviewed following defined triggering events, such as contract renewal or expiration, changes in service scope, ownership, or access, material technology changes, or significant incidents. Findings should be incorporated into procurement specifications, contract terms, technical standards, and operational procedures, as appropriate.

Cloud and Third-Party Services

Cloud-hosted and third-party services are increasingly used to support IBR monitoring, analytics, fleet management, and, in some cases, operational control functions. When these services interface with IBR operational environments, they introduce external dependencies that must be managed with the same rigor as on-premises systems. Cyber security responsibilities for cloud services are shared between the provider and the entity using the service, and security outcomes depend heavily on how those services are configured and governed. The following practices are strongly advised to manage risk of third-party services usage including cloud service providers (CSP) in association with IBR facilities:

- **Evaluate cloud and third-party services prior to operational integration.** Entities should assess the cyber security risk of cloud-hosted platforms and third-party services before they are integrated into IBR operations. Evaluations should consider the function performed, data handled, connectivity required, and potential impact of compromise or loss of availability.
- **Understand and address shared responsibility boundaries.** Entities should clearly identify which security responsibilities are managed by the service provider and which remain the responsibility of the asset owner or operator. Customer-managed responsibilities, such as user access, account configuration, data protection, and interface security, should be explicitly addressed. The allocation of responsibilities and the process for periodic review should be documented in contracts, service agreements, responsibility matrices, or governed procedures, as appropriate. Entities should also require service providers to identify material subcontractors and supplier dependencies and to manage those dependencies in a manner consistent with the entity's security expectations.
- **Require evidence of security governance and independent assessment.** Cloud and third-party providers supporting IBR operations should demonstrate that they maintain formal cyber security programs and undergo periodic independent security assessments. Evidence of established security governance helps reduce uncertainty but does not replace risk management by the entity using the service.
- **Define contractual expectations for data protection and incident notification.** Agreements with cloud and third-party providers should address data ownership, data handling and retention, and notification obligations for security incidents that could affect IBR operations or data. Entities should retain the ability to respond rapidly to provider-side security events.
- **Protect connectivity and access to cloud-based services.** Access to cloud platforms that support IBR operations should be restricted, authenticated, encrypted, and monitored. Interfaces used for operational control or telemetry exchange should be treated as part of the IBR attack surface and protected accordingly. Cloud-hosted services and vendor-managed assets should use dedicated interfaces, security zones, or other segmentation appropriate to their risk and should not create broad or direct connectivity into entity OT networks. See [Chapter 5](#) for more additional network segmentation guidance.
- **Account for service resilience and recovery capabilities.** Entities should consider the availability, redundancy, and recovery capabilities of cloud and third-party services that support IBR operations. Loss of service availability, regardless of cause, can have operational and security implications that should be understood and planned for.
- **Reassess cloud and third-party risk on an ongoing basis.** Cyber security risk associated with cloud and third-party services evolves over time. Entities should periodically review service configurations, provider posture, and emerging threats to ensure continued alignment with IBR operational risk tolerance.

Ongoing Vendor and Third-Party Risk Management

Supply chain and third-party cyber security risk continues throughout the operational life of an IBR facility. Vendor access, software dependencies, and support relationships evolve over time, and unmanaged changes can introduce new attack paths. Entities should maintain ongoing oversight of third-party relationships and access to ensure that security expectations remain effective as conditions change. Vendor and third-party reviews may occur on a scheduled basis or in response to milestone events, including contract renewals, changes in ownership or control, or material changes to access, services, provider architecture, new technology capabilities, or system integration. The following practices are recommended for ongoing risk management:

- **Maintain an inventory of third-party access and dependencies.** Entities should track vendors, contractors, and service providers with access to IBR systems, including the type of access granted, systems affected, and duration of access. This inventory should include both on-site and remote access paths.
- **Periodically review and remove unnecessary access.** Third-party accounts, credentials, and access paths should be reviewed on a regular basis and promptly removed when no longer required. Access granted for commissioning, warranty support, or temporary maintenance activities should be timebound and closed once the activity is complete.
- **Coordinate patching and updates with vendors.** Entities should maintain processes to receive notification of vendor-provided software and firmware updates and to evaluate and apply those updates in a timely manner. Where immediate application is not feasible due to operational constraints, compensating measures should be considered until updates can be deployed.
- **Monitor third-party activity within IBR environments.** Vendor access to IBR systems should be logged and monitored in the same manner as internal access. Monitoring should support detection of anomalous activity, unauthorized changes, or use outside of approved windows.
- **Establish communication and escalation expectations with critical vendors.** For vendors that provide core IBR equipment, platforms, or services, entities should maintain defined channels for cyber security communication, including notification of vulnerabilities or incidents and coordination during response activities.
- **Retain the ability to suspend or terminate third-party access.** Entities should maintain technical and procedural capability to rapidly restrict or disable vendor access to IBR systems in response to security concerns, incidents, or changes in vendor risk posture.
- **Reassess vendor risk as conditions change.** Vendor risk should be revisited over time to account for personnel changes, corporate restructuring, changes in service scope, and emerging threats that may affect the security of IBR operations.

Geographic and Jurisdictional Sourcing Considerations

The sourcing of hardware, software, and services for IBR environments can introduce risk related to manufacturing origin, jurisdictional control, and foreign access to systems or data. Because IBR facilities often rely on software-defined control, remote connectivity, and repeated deployment of common platforms, sourcing decisions for critical components can have fleet-wide operational and security implications. It is recommended that the following practices be broadly incorporated:

- **Incorporate sourcing considerations into supply chain risk assessments.** Entities should consider country of origin, jurisdictional oversight, and support location for critical IBR components and services as part of overall supply chain risk management.

- **Account for advisories and restrictions.** Where applicable, entities should consider relevant government, regulatory, and industry advisories,³ restrictions, or prohibitions related to high-risk products, vendors, or technologies and incorporate those considerations into procurement and approval processes.
- **Understand data location and access implications.** For third-party or cloud-based services supporting IBR operations, entities should understand where operational data is stored and which parties may have legal or administrative access to that data based on jurisdiction.
- **Avoid single-region dependency for critical functions where practicable.** Reliance on a single supplier or region for critical IBR control, monitoring, or communications functions can increase systemic risk and should be evaluated accordingly.
- **Apply enhanced scrutiny where sourcing risk is elevated.** Where higher sourcing risk is identified, entities should consider additional validation, contractual controls, or operational safeguards to reduce exposure.

³ Stay informed on alerts and advisories issued by organizations such as the U.S. Department of Energy (DOE), the Cybersecurity and Infrastructure Security Agency (CISA), the Department of Homeland Security (DHS), the Electricity Information Sharing and Analysis Center (E-ISAC), and NERC regarding high-risk vendors, components, or emerging supply chain concerns.

Chapter 3: Identity and Access Management

Identity and access management controls are a primary safeguard against unauthorized interaction with IBR systems. Because IBR environments commonly support remote access, third-party support, and distributed operations, weaknesses in identity controls can quickly translate into loss of visibility or control across multiple assets. Entities should establish and maintain identity and access management practices that ensure only authorized users and services can access IBR systems, and only to the extent necessary for their role. This scope includes identities and service accounts used by cloud-hosted platforms, vendor portals, automated analytics, and AI-enabled operational support tools. The following key practices are recommended to be followed for identity and access management of all IBR assets:

- **Require unique identification for all users and service accounts.** All personnel and non-human accounts accessing IBR systems should be uniquely identifiable. Shared or generic accounts should not be used, as they prevent accountability and hinder timely removal of access when no longer required.
- **Enforce strong authentication for interactive access.** Interactive access to IBR systems, particularly remote access, should require multi-factor authentication. Authentication mechanisms should ensure that compromise of a single credential (e.g., a lone password) is insufficient to gain access to control, monitoring, or configuration functions.
- **Apply least privilege and role-based access control.** Access permissions should be limited to the minimum required for assigned responsibilities. Role-based access control should be used where supported to define and manage access consistently across users and systems.
- **Manage credentials and authenticators securely.** Default credentials on IBR devices and applications should be removed or disabled prior to commissioning. Where supported, stronger authentication mechanisms such as cryptographic keys, certificates, or hardware-backed credentials (e.g., Secure Shell (SSH) key-based authentication or certificate-based device identity) should be used in place of password-only authentication. Authentication secrets should be stored and managed using secure mechanisms, and credentials and tokens should be reviewed periodically and revoked promptly when no longer required. Privileged and emergency access processes should avoid dependence on a single individual, authenticator, or credential while preserving individual accountability. Entities should periodically recertify user, service, and privileged access and remove or adjust access that is no longer justified.
- **Control and integrate third-party identities.** Vendor and contractor access should be subject to the same identity and authentication requirements as internal users. Third-party access should be individually assigned, timebound where feasible, and removed promptly when work is complete or contracts end.
- **Log and monitor authentication and access activity.** IBR systems and supporting platforms should log authentication events, access attempts, and privilege changes. Logs should be reviewed or monitored to detect anomalous or unauthorized activity, and entities should maintain the ability to respond quickly to suspected misuse of credentials.

Chapter 4: Remote Access and Network Connectivity

Remote access and external network connectivity are integral to IBR operations, supporting monitoring, maintenance, vendor support, and centralized control. These same capabilities also represent a primary attack path into IBR environments. Entities should treat all remote connectivity as a high-risk function and design, implement, and govern it accordingly. The following practices are recommended:

- **Require secure remote access by default.** All remote access to IBR systems should use encrypted communications, strong authentication, and explicit authorization. Unsecured or weakly protected remote access methods, including direct device exposure or password-only access, should not be used.
- **Enforce multi-factor authentication for interactive remote access.** Interactive remote access by personnel should require multi-factor authentication to ensure that compromise of a single credential does not result in unauthorized access.
- **Differentiate interactive access from machine-to-machine communications.** Interactive user access and automated system-to-system communications should be identified and protected using appropriate controls. Interactive access should be tightly governed and monitored, while machine-to-machine communications should be authenticated, encrypted, and restricted to defined endpoints and functions. Persistent machine-to-machine connections should use defined session timeouts, keepalive behavior, reauthentication or certificate renewal, and termination or fail-safe conditions appropriate to the protocol and operational need.
- **Use brokered or mediated access for interactive remote sessions.** Remote interactive access to IBR environments should be routed through owner-controlled access points, such as secure gateways or jump hosts, that enforce authentication, authorization, and logging. Direct remote connections into IBR control networks should be avoided.
- **Restrict remote access to defined systems and functions.** Remote users should be granted access only to the specific systems and functions required to perform approved tasks. Broad network-level access should not be provided where more granular controls are available.
- **Govern vendor and OEM remote access explicitly.** Vendor and third-party remote access should occur only through approved access methods and under defined conditions. Persistent or always-on vendor connections should be avoided unless operationally necessary and explicitly approved. Vendor access should be timebound, monitored, and subject to immediate revocation when no longer required. Approval should encompass any vendor-provided remote access tool and any cloud or subcontracted service on which that tool relies. Entities should evaluate provider dependencies, data flows, and network paths before use.
- **Account for cross-border remote access risk.** Remote access originating outside the local jurisdiction should be identified and evaluated for additional risk, including legal, regulatory, and operational considerations. Where elevated risk exists, additional safeguards or restrictions should be applied. Entities should consider denying access from jurisdictions that exceed established risk tolerance and should apply the same evaluation to managed service provider personnel and service locations.
- **Maintain visibility and control over active remote sessions.** Entities should be able to identify active remote connections to IBR systems, monitor session activity, and terminate access when necessary. Logging of remote access activity should support detection, investigation, and response to unauthorized or anomalous behavior. Where possible, entities should implement automation for these controls to more effectively manage remote session risk.

- **Document and enforce remote access expectations.** Remote access requirements should be defined in policy or procedures that establish who may access IBR systems remotely, under what conditions, using which methods, and with what oversight.

Chapter 5: Network Architecture and Segmentation

Network architecture and segmentation practices for IBR facilities vary widely based on site size, age, operational requirements, and design maturity. Some facilities may have limited ability to implement complex segmentation or layered architectures due to equipment capabilities, vendor constraints, or operational considerations. The recommendations in this section are intended to describe sound security outcomes and architectural principles rather than prescribe a single required design.

Entities should apply these practices using a risk-informed approach, considering operational impact, protocol behavior, and system limitations. Where full implementation is not feasible, entities should prioritize measures that reduce the most significant risks and pursue incremental improvements over time. All changes to network architecture and traffic controls should be engineered, tested, and validated to ensure that real-time control, protection, and monitoring functions are not adversely affected.

For purposes of this guideline, a security zone is a logical grouping of systems with similar function and security requirements (e.g., inverter control equipment, protection and automation equipment, or site operations support systems). A conduit is the controlled communication path between zones. Conduits are typically implemented using firewalls, security gateways, routers, or application proxies that enforce explicit limitations on what traffic is permitted between zones, including allowed protocols, ports, endpoints, and directionality.

The following practices are organized into baseline, enhanced, and advanced tiers. Baseline practices represent a minimum set of segmentation outcomes that should be achievable for most IBR facilities. Enhanced practices represent additional measures that further reduce risk and may be appropriate for higher-impact sites, newer designs, or facilities undergoing significant upgrades. Advanced practices offer rare or situational practice considerations for per-network or per-facility consideration.

Baseline Practices

- **Separate operational networks from the internet and corporate IT networks.** Networks supporting inverter control, plant controllers, human-machine interfaces (HMI), and protection systems should not be directly reachable from the internet. Connectivity to enterprise networks should occur only through controlled boundary devices.
- **Establish defined network segments for major functions.** At minimum, entities should separate IBR control functions from operations support functions and external communications functions using virtual local area networks (VLAN), access control lists (ACL), or firewalls, as supported by site equipment.
- **Allow list required communications and block all other traffic by default.** Boundary rules should restrict traffic to required protocols, endpoints, and directions. Unnecessary services and protocols should be denied.
- **Secure field communications over untrusted networks.** Communications traversing carrier, wireless, or third-party networks should be encrypted and authenticated using mechanisms appropriate to the use case (for example, site-to-site virtual private networks (VPN) or mutually authenticated transport layer security (TLS)).
- **Harden and control protocol converters and gateways.** Protocol converters, data concentrators, and communications gateways should be treated as high-risk assets. These devices should be hardened, updated, restricted to required communications, and monitored where feasible.

Enhanced Practices

- **Define security zones and controlled conduits.** Entities should group systems into zones based on function and risk and define controlled communication paths between zones. Conduits should enforce explicit limitations on protocols, endpoints, and directionality.
- **Use a site demilitarized zone (DMZ) for externally facing services and broker functions.** Systems that interface with enterprise networks, remote access services, or external data exchanges should be placed in a site DMZ or dedicated boundary segment rather than within the control zone.
- **Avoid direct bridging between trust zones.** Where feasible, communications should terminate at boundary systems (e.g., proxies, brokers, or gateways) rather than permitting direct end-to-end connectivity across zones.
- **Secure redundant communication paths equivalently.** Backup communications (e.g., cellular failover) should be subject to the same security protections as primary links and should not introduce weaker authentication or broader exposure.
- **Align segmentation boundaries with monitoring points.** Segmentation boundaries should support visibility into allowed and denied traffic. Entities should use these points to support detection of anomalous traffic and policy violations.

Advanced Practices

- **Implement internal micro-segmentation to limit lateral movement.** Entities should restrict east-west traffic within facilities to limit propagation if a device is compromised. Controls may include internal firewalls, ACLs, private VLANs, or host isolation features.
- **Apply protocol-aware filtering where operationally feasible.** Where supported and validated, industrial firewalls or gateways should enforce protocol-level restrictions to limit commands and functions to those required for operations.
- **Use mediated boundary services and protocol breaks for critical pathways.** For high-risk or high-impact interfaces, use application-layer gateways, brokers, or other boundary services that terminate and re-establish communications across zones rather than forwarding traffic transparently.
- **Control and minimize dual-homed devices and unmanaged wireless connectivity.** Dual-homed systems should be avoided or strictly controlled to prevent bypass of segmentation boundaries. Wireless access should be segmented from control zones and protected using strong authentication and access restrictions.
- **Use unidirectional enforcement where only outbound data is required.** Where operational requirements allow one-way data flow (e.g., telemetry outward without inbound control), entities should consider unidirectional architectures to reduce exposure.

Internal Network Security Monitoring

Segmented network architectures create defined points where traffic can be observed and evaluated. Entities should consider using internal network security monitoring solutions designed for OT environments to provide visibility into network activity of IBR assets without disrupting operations.

For IBR facilities, monitoring approaches should prioritize passive methods that observe traffic through span ports, network taps, or mirrored interfaces rather than active scanning or polling of field devices. Many IBR

devices and controllers are sensitive to unexpected network traffic, and active discovery techniques can introduce operational risk.

OT-designed monitoring solutions can provide detection of anomalous communications, unauthorized devices, unexpected protocol use, and policy violations at network boundaries and within left to right traffic of segmented zones. When deployed at conduits, site gateways, or DMZ interfaces, these solutions can enhance detection while reinforcing segmentation controls.

In some cases, OT-designed internal network security monitoring solutions offer features to assist with asset discovery, software and firmware identification, and detection of configuration changes gathered through the observation of normal network communications. For IBR environments where direct querying of devices is limited or undesirable, passive monitoring can improve asset visibility and highlight changes without introducing operational risk that could potentially result from automated asset management tools that strictly rely on active scanning or querying.

Chapter 6: Asset Management and Configuration Control

Effective cyber security for IBR facilities depends on maintaining accurate awareness and control of the hardware, software, and configurations that support operations. IBR environments often include a mix of vendor equipment, embedded devices, long-lived field assets, and site-specific integrations that evolve over time. Without disciplined assets, configuration, and change management, security controls degrade, visibility is lost, and risk accumulates quietly as systems drift from their intended state.

Asset management practices for IBR facilities must account for operational constraints, vendor dependencies, and the realities of maintaining geographically distributed sites with limited on-site staffing. The recommendations in this section are intended to establish consistent outcomes rather than prescribe specific tools or processes. Entities should apply these practices in a risk-informed manner by prioritizing the assets that support control, protection, communications, and external connectivity and validating changes to these assets to avoid unintended operational impact. The following asset management and configuration change management controls are recommended broadly for IBR assets:

- **Maintain an inventory of IBR assets and supporting components.** Entities should maintain an inventory of hardware and software used at each IBR facility, including inverters, plant controllers, HMIs, protection and automation devices, network equipment, communications devices, and supporting servers or virtual components. Inventory records should capture identifying and operationally relevant information such as device type, model, firmware or software version, network location, criticality, and responsible owner or vendor.
- **Keep asset inventories current as changes occur.** Asset inventories should be updated as equipment is installed, removed, replaced, or updated. Changes introduced during commissioning, maintenance, or troubleshooting should be reflected in the inventory to avoid loss of visibility over time.
- **Define and document baseline configurations for critical assets.** For devices that support control, protection, communications, or remote access, entities should establish approved baseline configurations that reflect secure and operationally appropriate settings. Baselines may include enabled services, network settings, access controls, firmware versions, and security-relevant parameters.
- **Manage configuration changes deliberately.** Changes to baseline configurations should be reviewed, approved, and documented prior to implementation where practicable. Configuration changes made to support troubleshooting or temporary operational needs should be tracked and either reverted or formally incorporated into the approved baseline. Change management processes should identify and evaluate proposed changes, including vendor actions, updates, replacements, and temporary troubleshooting changes, before implementation where practicable. Detected changes should be reviewed promptly to identify and address out-of-process activity.
- **Monitor for unauthorized or unintended configuration changes.** Entities should periodically review device configurations and settings to identify deviations from approved baselines. Reviews may be manual or automated and should focus on changes that could affect security, connectivity, or control behavior.
- **Manage patching and updates throughout the asset lifecycle.** Entities should maintain processes to evaluate and apply security patches and firmware updates for IBR assets in coordination with operational requirements. Where immediate patching is not feasible, compensating measures such as increased monitoring or network isolation should be considered until updates can be applied.

- **Verify authenticity of software and firmware updates.** Software and firmware updates should be obtained from trusted sources and verified prior to installation using available integrity checks or vendor-provided validation mechanisms.
- **Apply device hardening appropriate to IBR environments.** Devices should be configured to minimize unnecessary attack surface by disabling unused services, removing default credentials, and enabling supported security features. Hardening should consider operational constraints and vendor guidance to avoid impacting system reliability.
- **Collect logs and audit asset configurations regularly.** Security-relevant events such as authentication activity, configuration changes, and system status should be logged where supported. Periodic audits should confirm that accounts, permissions, and configurations remain aligned with current operational needs.
- **Plan for asset lifecycle and end-of-support conditions.** Entities should track vendor support timelines for hardware and software used in IBR facilities and plan for replacement, upgrade, or risk mitigation prior to end of support. Assets that can no longer receive security updates should be evaluated for isolation, enhanced monitoring, or retirement.
- **Maintain backups of configurations and critical data.** Configuration data and critical operational information should be backed up on a regular basis and stored securely. Backup processes should be tested periodically to confirm that restoration can be performed reliably during recovery or incident response activities.

Chapter 7: Information Classification and Protection

IBR facilities generate and rely on a wide range of technical, operational, and planning information. While much of this information may not fall under mandatory protected information categories, certain IBR-related data can present security or reliability risk if improperly disclosed, altered, or misused. Entities should differentiate IBR-related information based on whether it would enable unauthorized access, reveal security-relevant architecture, or materially increase the ability to disrupt operations. Because IBR operations rely heavily on digital commands, telemetry, remote access, and data exchange, integrity is often as consequential as confidentiality. Where feasible, entities should apply controls to prevent or detect unauthorized modification of control instructions, configuration data, setpoints, event records, and operational telemetry and should validate data integrity during recovery.

Currently, mandatory information protection requirements in NERC CIP apply to Bulk Electric System Cyber System Information (BCSI) associated with applicable high- and medium-impact BES cyber systems; most IBR facilities fall outside that scope. Certain categories of IBR information still warrant heightened handling based on content and context. Examples include inverter and plant controller configuration and setpoints, protection and automation settings, network architecture diagrams and access pathways, remote access configurations, operational telemetry and control data, high-resolution monitoring data such as phasor measurement unit (PMU) or event records, and planning or interconnection studies that describe system behavior or limits. In some cases, information may also qualify as Critical Energy Infrastructure Information (CEII) depending on content and use.

Entities should apply appropriate judgment when determining how IBR-related information is stored, shared, transmitted, and retained. Even where formal classification requirements do not apply, treating certain operational and technical information as sensitive supports defense-in-depth and reduces the likelihood that detailed system knowledge could be leveraged to compromise IBR assets or broader system reliability.

Chapter 8: Secure Communication Protocols and Telemetry

IBR facilities depend on continuous, often real-time communications to support monitoring, control, protection, and coordination with external systems. These communications may occur within the facility, between sites and control centers, or with third-party platforms such as DER management systems, market interfaces, or vendor support services. The security of these communication paths is critical, as unauthorized access, manipulation, or interception of control or telemetry data can directly affect system reliability and safety.

Many IBR environments continue to rely on legacy industrial communication protocols that were designed for reliability and interoperability rather than cyber security. These protocols often lack native encryption, authentication, or integrity protection, exposing communications to risks such as credential capture, command injection, or data manipulation. At the same time, operational requirements, latency sensitivity, device resource constraints, and interoperability with third-party systems or legacy equipment can limit the ability to adopt modern secure protocols universally.

The recommendations in this section recognize these competing factors. Entities should understand the communication protocols in use across their IBR environments, assess where security weaknesses exist, and apply appropriate protections based on risk and operational impact. Where secure protocol options are available, they should be used. Where limitations exist, entities should implement compensating controls, document residual risk, and plan for incremental improvement as technology and vendor support evolve. Entities should adopt the following recommendations regarding IBR assets protocol security:

- **Identify and document communications protocols in use.** Entities should maintain awareness of what protocols are used between inverters, controllers, gateways, and external systems. Understanding protocol behavior, including timing sensitivity, authentication capability, and data formats is essential to applying appropriate protections. Protocol and interface inventories should additionally include cloud application programming interfaces (API), vendor platforms, and data exchanges used by analytics or AI-enabled services, including the parties that host or manage each interface.
- **Use secure protocol variants wherever available.** Where supported, use protocols that provide encryption and authentication. Examples include SSH instead of Telnet, HTTPS instead of HTTP, SFTP or FTPS instead of FTP, SNMPv3 instead of SNMPv1/v2c, and DNP3 Secure Authentication (SAv5) or IEC 62351-protected variants of International Electrotechnical Commission (IEC) protocols for control and telemetry. These options protect credentials and command traffic from interception or tampering.
- **Use encrypted and authenticated tunnels for untrusted links.** Any telemetry or control traffic that traverses public, carrier, or third-party networks should be protected using encryption (for example, TLS or IPsec) with mutual authentication between endpoints. Site-to-control-center connections should use VPN tunnels or equivalent secure channels, ensuring that both confidentiality and integrity are preserved.
- **Apply compensating controls where secure protocols are not supported.** When devices cannot support secure protocols due to performance or hardware limitations, use external gateways or firewalls to encapsulate or mediate the communication securely. For instance, a site gateway can terminate secure VPN connections on behalf of legacy inverters that only speak Modbus/TCP or HTTP.
- **Restrict and monitor insecure or legacy protocol use.** Legacy plaintext services such as Telnet, HTTP, FTP, or TFTP should be disabled where possible. If such protocols must remain active for

compatibility reasons, restrict them to isolated network segments, enforce strict access controls, and monitor their use for anomalies.

- **Secure telemetry and monitoring channels.** Telemetry between IBR sites and control centers should be authenticated to verify source integrity and protect against modification in transit. Where possible, apply encryption equivalent to control system traffic and use private or VPN paths for backhaul connections.
- **Identify and document embedded communications capabilities.** Entities should verify and document wired and wireless interfaces present in inverters and supporting field equipment, including cellular, Wi-Fi, Bluetooth, optional or disabled modules, and other radio technologies. Verification should not rely solely on manufacturer documentation and may include procurement and acceptance records, supported configuration data, external observation, and appropriately authorized passive wireless assessment.
- **Control embedded communications modules and conduct inspections safely.** Interfaces or modules that are not required should be disabled or, where appropriate, removed. Those retained should be protected using appropriate authentication, segmentation, private access point names, VPNs, or equivalent controls and monitored for unauthorized use. Any inspection or removal requiring an inverter enclosure or internal compartment to be opened should be performed only by personnel qualified and authorized for the equipment, consistent with applicable site electrical-safety and manufacturer procedures, including controls for de-energization, lockout/tagout, personal protective equipment, and stored energy.
- **Plan for incremental improvement and technology refresh.** Entities should track protocol capabilities and vendor roadmaps to identify when secure variants or firmware support become available. Where modernization is not yet feasible, maintain compensating network protections until upgrades can be implemented.

Chapter 9: Incident Response and Recovery Preparedness

Cyber incidents in IBR environments do not always look like a clean “IT outage.” They may present as loss of telemetry, unexpected plant controller behavior, unexplained inverter trips, setpoint changes that do not match operator intent, or instability that resembles equipment malfunction. Response actions must protect personnel safety and reliable operation first while preserving the ability to contain the event, determine what changed, and restore systems to a known-good state.

IBR response also has a scaling problem: Common architectures, shared vendor platforms, and centralized fleet tooling can turn a single compromise into a multi-site issue. Dependencies on telecommunications providers, distributed energy resource management system (DERMS) or fleet monitoring platforms, and vendor remote support can complicate both containment and recovery. Plans should assume degraded communications, limited on-site staffing, and the possibility that vendor tools or cloud portals are part of the affected path.

The recommended practices below are aimed at reflecting the reality that IBR organizations operate at different maturity levels and with different site capabilities. Baseline practices establish a minimum response capability that reduces confusion and delays during an event. Enhanced practices build additional resilience and speed and are appropriate for higher-impact sites, fleet operators, or entities with greater operational dependency on remote connectivity and third parties.

Baseline Incident Response and Recovery Practices

- **IBR-specific response procedures and decision authority.** Entities should maintain IBR-specific procedures that define who can take operational actions (i.e., disable remote access, isolate a site, curtail output, or place a plant into a safer operating mode), and under what conditions.
- **Clear incident triggers and escalation criteria.** Entities should define operational indicators that require escalation, including unexplained loss of telemetry, repeated inverter trips without clear equipment cause, unexpected control mode changes, unauthorized account activity, abnormal remote access behavior, or evidence of configuration or firmware change. Because dispersed sites may be monitored by a small number of personnel or through mobile or cloud interfaces, monitoring and escalation processes should consider fleet-level response options (e.g., aggregating signals across sites) to reduce dependence on a single individual or device.
- **Immediate containment “levers” that do not require onsite action.** Entities should be able to rapidly disable vendor remote access, revoke third-party credentials, restrict remote connectivity to a site, and isolate the site DMZ or external gateways, while preserving minimum operational visibility where possible.
- **Playbooks for common IBR scenarios.** Entities should maintain step-by-step playbooks for at least suspected credential misuse/remote intrusion, suspected setpoint or mode manipulation, loss of communications with indicators of compromise, compromise of a gateway/protocol converter, ransomware impacting site operations support systems, and compromise of cloud or third-party platforms supporting monitoring or control.
- **Cross-functional coordination paths and out-of-band communications.** Entities should maintain current contact methods and escalation paths across operations, cyber response, field support, vendors, and telecommunications providers. Plans should include out-of-band communications methods that remain usable during a network outage or containment action.

- **Minimum evidence preservation expectations.** Entities should preserve key artifacts when feasible before rebuilding systems, such as logs, configuration snapshots, and relevant event timelines. Evidence preservation should be practical and not delay safety-driven containment or restoration.
- **Backups and restore capability for control-relevant configurations.** Entities should maintain secure backups for plant controller configurations, gateway and firewall configurations, critical server images where applicable, and known-good parameter sets required to safely restore operations. Backups should be protected from ransomware and tampering and tested periodically.
- **Restoration validation before return to normal operation.** Recovery steps should include validation that access paths, accounts, configurations, and communications flows match approved baselines and that operational behavior is expected (e.g., command pathways, limits, and telemetry integrity).
- **External notification and reporting awareness.** Entities should maintain a process to determine whether an event triggers required external notifications or reporting based on entity role and event impact, including reliability event reporting and Department of Energy (DOE) disturbance reporting where applicable.

Enhanced Incident Response and Recovery Practices

- **Fleet-level response coordination and cross-site correlation.** Entities operating multiple IBR sites should maintain the ability to identify patterns across the fleet (e.g., common alarms, common access events, shared vendor touchpoints) and to coordinate containment actions consistently across sites.
- **Predefined degraded operations modes and “safe state” actions.** Where supported by plant design and operating agreements, entities should define preapproved operational actions for suspected cyber events (e.g., intentional islanding where the facility is designed and authorized for it, restricting control to local mode, limiting setpoint change capability, or implementing temporary command gating), aligned with safety and reliability requirements.
- **Pre-staged recovery tooling and clean engineering workstations.** Entities should maintain clean, preconfigured laptops and offline recovery materials (e.g., diagrams, configs, firmware images, licenses where needed) to support site restoration without reliance on potentially compromised systems.
- **Golden configurations and integrity validation.** For critical components, entities should maintain known-good baselines and validate restoration using available integrity mechanisms (e.g., vendor signature validation, hashes, or controlled reimaging methods), particularly for gateways and controller platforms.
- **Spare parts and logistics planning for remote sites.** Entities should preplan availability of critical spares (e.g., key network devices, controller modules, gateway devices) and the logistics to deploy them rapidly to remote locations.
- **Vendor and telecom participation in incident response exercises.** For key vendors and communications providers, entities should establish expectations for incident-time support, participation in drills, and rapid coordination during provider-side security events.
- **Testing that includes operational decision-making under uncertainty.** Exercises should simulate conditions common to IBR incidents: partial telemetry, conflicting indicators, remote access uncertainty, and time pressure to protect reliability. Exercises should test both cyber actions (e.g., containment, recovery) and operational actions (e.g., curtailment, isolation, command restrictions).

- **Preparedness for IBR event reporting and data preservation.** Entities should be prepared to preserve relevant operational and disturbance data during large IBR events to support event analysis and reporting, recognizing that data may be overwritten or lost if not captured promptly.

Chapter 10: Conclusion

IBRs are now an essential component of BPS reliability, and their increasing scale, connectivity, and operational complexity introduce cyber security considerations that differ from traditional generation assets. The practices described in this guideline are intended to help entities better understand and manage those risks by applying practical, risk-informed cyber security measures that reflect the operational realities of IBR environments. While not all practices will be feasible for every facility, even incremental improvements can reduce exposure to cyber events that may affect safety, availability, and system reliability.

This guideline is advisory in nature and is intended to support informed decision-making rather than prescribe mandatory requirements. By thoughtfully applying the recommendations in a manner appropriate to their assets, architecture, and operational constraints, entities can strengthen the resilience of IBR facilities and contribute to BPS reliability and security. As IBR technologies, operational models, and threat conditions continue to evolve, this guideline is expected to be reviewed and updated to reflect industry experience, emerging risks, and lessons learned over time.

Appendix A: Contributors

NERC gratefully acknowledges the contributions and assistance of the following industry experts in the preparation of this guideline (see [Table A.1](#)).

Table A.1: Contributors	
Name	Entity
Alejandro Gonzalez	Guidehouse
Alekhya Avadhanula	EPRI
Barry Jones	PG&E
Bheshaj Krishnappa	SEIA
Birk Jones	Sandia
Brandon L Weese	AEP
Brian Roberson	Recurrent Energy
Brian Seal	EPRI
C. Nathan Hodge	Southern Company
Carver Powers	Utility Services
Christopher Landry	Entergy
Christopher Walcutt	DirectDefense
Dan Goodlett	NERC
David Sopata	ReliabilityFirst
Emma M. Stewart	INL
Gang Fong	Copia Power
Gregg Groshon	Arevon Energy
Hemanta Sinha	Nexamp
Jen McCabe-de Achaval	Utility Services
John Franzino	GridSec
Kristine Martz	EEI
Larry Collier	NERC
Lee Felter	MRO
Mahmood Safi	Vistra
Machelle Ramos	Liberty Utilities
Mike Lamb	Dominion Energy
Mohammed Banajah	BBA Consultants
Morgan King	WECC
Olivia Olson	Shome Power
Patricio Gomez	Radian Generation
Ramneek Dimen	Recurrent Energy
Ranjan Banerji	AWS
Sai Ram Ganti	EPRI

Table A.1: Contributors

Name	Entity
Thomas Peterson	GE Vernova
Tobias Whitney	Cumulys
Travis McKee	Arevon Energy
Xavier Francia	EPRI

Appendix B: Guideline Information and Revision History

Guideline Information	
Category/Topic: Inverter Based Resources Architecture	Reliability Guideline/Security Guideline/Hybrid: Security Guideline
Identification Number: [NERC use only]	Subgroup: SITES

Revision History		
Version	Comments	Approval Date
1.0	Approved by the RSTC	XX/XX/XXX

Appendix C: Metrics

Pursuant to the Commission's Order on January 19, 2021, North American Electric Reliability Corporation, 174 FERC ¶ 61,030 (2021), reliability guidelines shall now include metrics to support evaluation during triennial review consistent with the RSTC Charter.

Baseline Metrics

All NERC reliability guidelines include the following baseline metrics:

- BPS performance prior to and after a reliability guideline as reflected in NERC's *State of Reliability* report and long-term reliability assessments (e.g., *Long-Term Reliability Assessment* and seasonal assessments)
- Use and effectiveness of reliability or security guidelines as reported by industry via survey
- Industry assessment of the extent to which a reliability guideline is addressing risk as reported via survey

Specific Metrics

The RSTC or any of its subcommittees can modify and propose metrics specific to the guideline to measure and evaluate its effectiveness, listed as follows:

- No additional metrics are proposed specific to the content of this reliability guideline.

Effectiveness Survey

On January 19, 2021, FERC accepted the proposed NERC approach for evaluating reliability guidelines. This evaluation process takes place under the leadership of the RSTC and includes the following:

- Industry survey on effectiveness of reliability guidelines;
- Triennial review with a recommendation to NERC on the effectiveness of a reliability guideline and/or whether risks warrant additional measures; and
- NERC's determination whether additional action might be appropriate to address potential risks to reliability considering the RSTC's recommendation and all other data within NERC's possession pertaining to the relevant issue.

NERC is asking entities that are users of reliability and security guidelines to respond to the short survey provided in the link below.

[Guideline Effectiveness Survey](#)