DISCLAIMER

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. Reference herein to any social initiative (including but not limited to Diversity, Equity, and Inclusion (DEI); Community Benefits Plans (CBP); Justice 40; etc.) is made by the Author independent of any current requirement by the United States Government and does not constitute or imply endorsement, recommendation, or support by the United States Government or any agency thereof.

Navigating U.S. Standards and Regulation for Digital Energy Systems

INL/RPT-25-89608

Center for Securing Digital Energy Technology

Standards and Regulation Risk Mapping

FEBRUARY 2026

Idaho National Laboratory

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy

INL/RPT-25-89608

Navigating U.S. Standards and Regulation for Digital Energy Systems

Standards and Regulation Risk Mapping

FEBRUARY 2026

Idaho National Laboratory
National & Homeland Security
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Page intentionally left blank

CONTENTS

ACRONYMS

AMI	Advanced Metering Infrastructure
APT	Advanced Persistent Threat
BES	Bulk Electric System
BESS	Battery Energy Storage Systems
C2M2	Cybersecurity Capability maturity Model
CESER	Office of Cybersecurity, Energy Security, and Emergency Response
CIE	Cyber-Informed Engineering
CIP	Critical Infrastructure Protection
DER	Distributed Energy Resource
DERCF	Distributed Energy Resource Cybersecurity Framework
DOE	U.S. Department of Energy
FBI	Federal Bureau of Investigation
FERC	Federal Energy Regulatory Commission
GAO	Government Accountability Office
GRIP	Grid Resilience and Innovation partnerships
IBR	Inverter-based Resource
IEEE	Institute of Electrical and Electronics Engineers
INL	Idaho National Laboratory
IOU	Investor-owned Utility
IPP	Independent Power Producer
MVA	Mega Volt-amperes
NARUC	National Association of Regulatory Utility Commissioners
NERC	North American Electric Reliability Corporation
NFPA	National Fire Protection Association
NLR	National Laboratory of the Rockies
O&P	Operations & Planning
OT	Operational Technology
PUC	Public Utility Commission
SEO	State Energy Office
U.S.	United States

Page intentionally left blank

Navigating United States Standards and Regulation for Digital Energy Systems

Standards and Regulation Risk Mapping

1. INTRODUCTION

United States (U.S.) utilities are expanding digital energy infrastructure, including battery energy storage systems (BESS), advanced metering infrastructure (AMI), and advanced grid-control systems, to improve efficiency, reliability, and capacity amid growing electricity demand. These deployments are regulated by intersecting frameworks of federal, state, and voluntary standards covering cybersecurity, communication protocols, safety, interconnection, and reliability. The purpose of this brief is to give utilities, regulators, and project developers a concise overview of the current landscape of standards and regulations in the U.S., identify gaps between compliance and real-world risk coverage, and recommend steps to improve security of digital-energy infrastructure. The scope of this report focuses on the categorical types of standards (federal and state regulation, voluntary consensus standards, and utility-driven standards) rather than on specific technologies.

Many industry standards designed to secure digital energy infrastructure technologies are voluntary or self-attested, creating compliance gaps. Utilities may be compliant yet face potential cybersecurity or safety risks due to gaps between compliance requirements and comprehensive security practices. Small municipal utilities and cooperatives are especially at risk as they often lack financial or expert resources to interpret and implement complex standards, whereas large investor-owned utilities may create bespoke requirements and vendor requirements with manufacturers. This report is intended for utilities and grid operators pursuing federal or state energy grants, including those participating as subrecipients. It is also relevant to State Energy Offices (SEOs), public utility commissioners, regulators, equipment manufacturers, and service providers. The brief outlines applicable standards and highlights where additional risk controls or oversight may be needed.

2. DIGITAL ENERGY TECHNOLOGY IS OUTPACING SECURITY STANDARDS

Cyber risk to the U.S. electric grid is often discussed in theoretical terms; however, historic events show that cyberattacks on energy assets are real and growing. The North American Electric Reliability Corporation (NERC) notes that digital threats are increasing in frequency and sophistication and are benefiting from an increased attack surface as the grid becomes more digitized [1]. This expanding threat surface reflects broader trends: smart meters, inverters, distributed controllers, and other variable energy resources now connect directly to the internet or vendor-managed platforms. These technologies can be outside of mandatory cybersecurity regulations such as NERC Critical Infrastructure Protection (CIP), leaving them dependent on voluntary best practices or vendor-defined controls. UL Solutions warns that many digitally connected energy assets, particularly smaller distributed installations, often lack robust cybersecurity standards and are often deployed with minimal access controls [2].

These concerns are reflected in recent exposure data. In June 2025, researchers identified approximately 35,000 internet-exposed solar power management systems [3]. Many of these systems were directly reachable from the public internet, creating potential entry points into operational networks. Similar research has documented over 130,000 exposed solar monitoring services and more than 145,000 internet-exposed industrial control systems across 175 countries, highlighting the scale of grid-edge exposure [4, 5].

In addition to internet-exposed interfaces, communications devices are a common target for attackers. In 2023, a state linked advanced persistent threat (APT) group, known as Volt Typhoon, gained access to

a municipal electric utilities' network through an unpatched firewall vulnerability [6]. The adversaries pre-positioned in the network for over 300 days until the small utility was notified by the Federal Bureau of Investigation (FBI). The threat was quickly isolated and the managed service provider responsible for patching the firewall was terminated from working with the utility as a result. Even years earlier, a Utah-based independent power producer (IPP) experienced an exploit of a firewall vulnerability by an unknown threat actor. The incident caused denial-of-service conditions that disrupted communications with multiple generation sites for five-minute intervals over several hours. This event is regarded as the earliest documented cybersecurity case to cause a "disruption" within the U.S. power sector, according to the Department of Energy's definition [7]. Both incidents occurred at facilities that fell below NERC CIP cyber regulation levels, demonstrating that gaps in comprehensive application of standards leave openings that adversaries have proven they will find and exploit.

These trends demonstrate a growing mismatch between the pace of digital energy technology deployment and the maturity of the cybersecurity frameworks intended to govern it. Grid-connected technologies are being deployed faster than regulations can adapt. Many of these assets fall outside mandatory cybersecurity requirements and rely instead on voluntary controls, vendor defaults, or ad hoc operational practices. The result is a rapidly expanding class of digitally connected energy systems that are operationally critical but inconsistently secured, increasing the likelihood that common enterprise-grade vulnerabilities, such as exposed management interfaces, unpatched firewalls, and weak authentication, can translate into grid-relevant consequences. This gap between technological capability and enforceable security standards is now a defining characteristic of modern digital energy infrastructure and a central driver of systemic cyber risk.

3. LANDSCAPE OF U.S. STANDARDS & REGULATIONS

The standards and regulatory framework for digital energy infrastructure in the U.S. operates as a multi-layered system in which federal and state regulations intersect with voluntary industry best-practice standards and utility-specific policies. Understanding this landscape is essential for utilities planning digital energy projects, as interactions among these layers create both compliance requirements and critical protection gaps. The following overview describes the four-layer regulatory structure and establishes context for understanding the gaps analyzed in section four of this report.

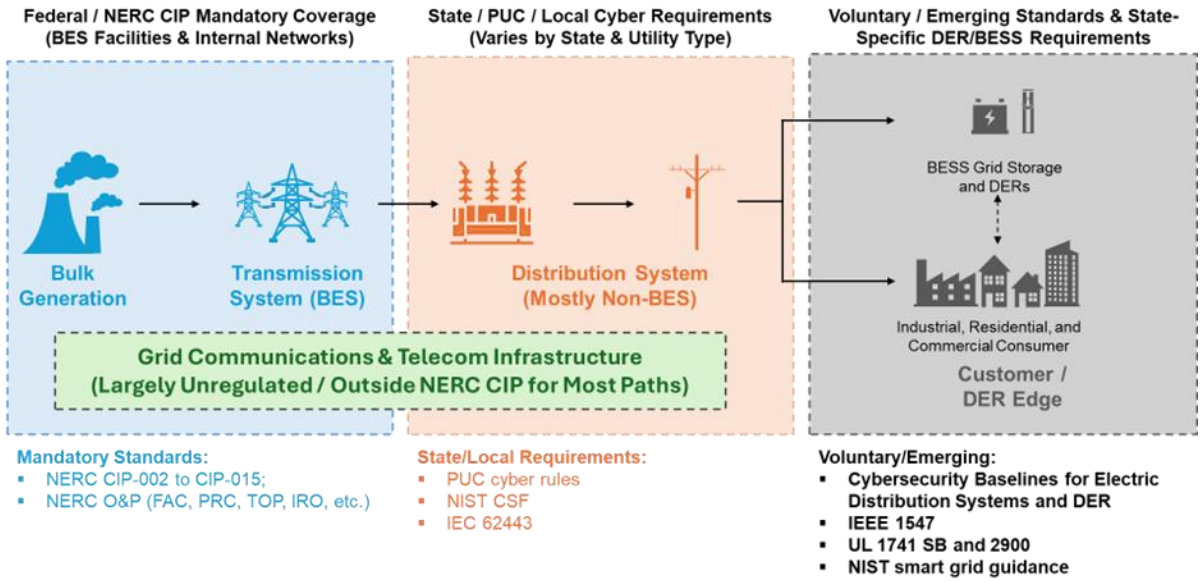

Figure 1: Regulatory coverage and standards landscape across generation, transmission, distribution, and grid-edge technologies.

3.1. Federal Policy & Mandatory Reliability Standards

At the federal level, the Federal Energy Regulatory Commission (FERC) oversees wholesale electricity markets and delegates authority to NERC to develop and enforce mandatory reliability standards for the Bulk Electric System (BES). NERC's Critical Infrastructure Protection (CIP) Standards establish mandatory cybersecurity requirements covering physical security, access controls, incident response, personnel training, and supply-chain risk management. However, NERC's CIP jurisdiction is limited to BES assets, which generally include transmission facilities at 100 kilovolts (kV) or higher and generation plants with a total aggregate of 75 mega volt-amperes (MVA) or higher. While NERC's Operations and Planning (O&P) standards now apply to specific inverter-based resources (IBR) at lower thresholds, including Generator Owner Category 2 IBRs at 20 megawatts (MW) or higher, these same resources currently have no corresponding CIP cybersecurity requirements.

NERC CIP was designed to regulate only BES assets, which include high-voltage transmission and large generation facilities. These assets represent approximately 10-20% of the total number of physical grid assets according to 2014 estimates published by the National Association of Regulatory Utility Commissioners (NARUC) (more current data is not publicly available) [8]. The remaining 80-90% of grid assets fall under state and local regulatory jurisdiction rather than mandatory federal oversight. While state regulations and voluntary standards address some distribution-level assets, coverage remains inconsistent and sometimes unenforceable. NERC CIP standards are enforceable through significant financial penalties for noncompliance, which can reach one million dollars per violation per day [9]. These standards comprehensively regulate cybersecurity and reliability within facility boundaries for BES assets, but three major categories remain outside mandatory federal cybersecurity oversight:

- **All grid communications equipment and infrastructure beyond the Electronic Security Perimeter are explicitly exempt.** This means routers, modems, circuits, and communications used for the control and monitoring of grid assets, though they carry critical operational data, are not required to meet any NERC CIP compliance requirements.
- **Distribution-level assets and most local infrastructure, including most digital energy resources, fall below BES voltage and power thresholds** and are not subject to mandatory federal cybersecurity standards. State-level cybersecurity requirements, where they exist, vary significantly in scope, stringency, and enforcement.
- **Newly registered IBRs that meet BES definition thresholds** (generally individual generators of 20MVA or aggregate resources larger than 75 MVA) [10], which NERC now regulates for reliability purposes through special Operations and Planning (O&P) standards, **currently have no CIP cybersecurity requirements**. While NERC plans to apply cybersecurity standards to these IBRs in the future, the implementation approach and timeline remain undetermined, potentially creating security gaps until they are put in place.

FERC has taken incremental steps to enable utility deployment of digital energy resources while also addressing emerging risks through various orders:

- In 2016, FERC issued Order No. 829 directing NERC to develop mandatory Reliability Standards to address supply chain risk management for control system hardware, software, and services supporting BES operations [11].
- In 2018, Order No. 850, FERC approved NERC's proposed CIP-013-1 Supply Chain Risk Management standard, along with modifications to CIP-005-6 and CIP-010-3. These standards established the first mandatory supply chain cybersecurity requirements for high and medium impact BES Cyber Systems [12].
- In 2020, FERC Order 2222 enabled aggregated distributed energy resources (DERs) to participate in wholesale markets but explicitly defers interconnection authority to state and local jurisdictions

[13], reinforcing the boundary between federal oversight and state control over distribution-level assets where most DERs operate.

- In 2021, FERC approved NERC CIP-013-2, which broadened the requirements of the original standard to include Electronic Access Control or Monitoring Systems and Physical Access Control Systems associated with high and medium impact BES Cyber Systems [14]. Under CIP-013-2, responsible entities must develop, implement, and review supply chain cybersecurity risk management plans addressing vendor risk, procurement, and software integrity.
- In 2023, Order No. 893 approved CIP-003-9, which expanded supply chain and vendor electronic remote access security controls to low-impact BES Cyber Systems. This action closed a key gap left by earlier standards that focused only on high and medium-impact systems [15].
- In 2025, FERC directed NERC to explore modifications to the CIP standards to address emerging technologies, including virtualization and cloud computing environments [16]. NERC Projects 2023-09 and 2025-03 are underway to ensure the CIP framework supports secure and compliant use of these technologies.

While these orders expand scope and technical requirements for mandatory critical infrastructure standard coverage across the BES spectrum, they still do not extend federally required protections to distribution-level assets or grid communications infrastructure that fall outside the BES definition.

The Department of Energy (DOE) provides voluntary, non-regulatory guidance through frameworks such as the Cybersecurity Capability Maturity Model (C2M2) [17], the National Laboratory of the Rockies (NLR) DER Cybersecurity Framework (DERCF) [18], the Supply Chain Cybersecurity Principles [19], and the National Cyber-Informed Engineering (CIE) Strategy [20]. C2M2 offers a maturity model for assessing cybersecurity capabilities, while DERCF provides DER-specific guidance. The Supply Chain Cybersecurity Principles, released in 2024, establish best practices for both suppliers and end users to strengthen cybersecurity across energy-sector supply chains. CIE promotes a "security-by-design" approach to integrate cybersecurity considerations into system engineering from the earliest design stages. While these tools offer valuable benchmarks for utilities seeking to improve security practices beyond minimum compliance, they carry no enforcement mechanism and rely entirely on voluntary adoption.

3.2. State Regulation & Public Utility Commission (PUC) Actions

While federal standards govern the BES, states have jurisdiction over distribution-level infrastructure where most digital energy resources operate. This authority has not translated into widespread equal adoption of cybersecurity requirements. In January 2025, the U.S. DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER), working with NARUC, developed cybersecurity baselines to strengthen protections for electric distribution systems and DERs [21]. These baselines serve as a resource for state PUCs, utilities, and distribution asset operators. However, they are voluntary frameworks rather than enforceable regulations, and states may adopt, modify, or ignore them at their discretion. As of 2024, at least seven states have adopted Institute of Electrical and Electronics Engineer (IEEE's) standard, IEEE 1547-2018, for DER interconnection requirements [22], and while the recently published IEEE 1547.3-2023 provides cybersecurity guidelines, these remain voluntary recommendations rather than mandatory requirements. Ultimately, IEEE standards do not have authority until enacted by law. Current implementations vary significantly by state and utility (discussed further in section 3.3 and section 4 below).

Public utility commissions have the legal authority to review utility cybersecurity practices and require disclosure of major breaches that impact reliability or safety. Some states have implemented task forces, reporting requirements, cost-recovery mechanisms, and open-records exemptions to improve cybersecurity [23]. However, state actions vary widely in scope and rigor, and resource constraints create uneven protection across states. A 2021 Government Accountability Office (GAO) report found that only

three of six surveyed states had dedicated cybersecurity personnel in PUCs, with officials noting they either lack resources to hire cybersecurity expertise or rely on utilities to manage their own security [24]. Since the GAO's 2021 report, state commissions have shown growing attention to cybersecurity, with some establishing dedicated offices or programs and others incorporating cybersecurity more formally into regulatory oversight. Resources such as NARUC's Critical Infrastructure Resource Repository [25] and its 2025 Essential Guide to Cybersecurity Resources [26] reflect this expanding engagement among PUCs.

State PUC authority generally applies most directly to investor-owned utilities (IOUs), resulting in more consistent cybersecurity expectations for that segment. Municipal utilities and electric cooperatives are often outside traditional PUC jurisdiction and are instead governed through local or member-based oversight, which limits the reach of commission-driven requirements. State Energy Offices (SEOs) can help bridge this gap by providing technical assistance and maturity-modeling support and by encouraging adoption of voluntary cybersecurity baselines. Nevertheless, because such support is not uniformly available or enforceable, cybersecurity coverage for electric cooperatives remains variable across states, contributing to a persistent standards gap beyond the BES.

3.3. Voluntary Standards

Voluntary consensus standards developed by industry organizations and standards development organizations form the technical foundation for digital energy infrastructure security and safety. These standards often represent industry best practices and carry weight with insurers, financiers, and equipment purchasers [27]. However, they become mandatory only when adopted by regulators into laws and regulations or required in procurement contracts.

Key voluntary standards categories include cybersecurity frameworks (NIST CSF, ISA/IEC 62443, UL 2941), safety and reliability standards (National Fire Protection Association (NFPA) 855, UL 9540/9540A, UL 1973, UL 1741), communication protocols (IEEE 2030.5, DNP3, SunSpec Modbus), and interconnection standards (IEEE 1547 series). The DER Cybersecurity Standards Library, developed by NLR, Idaho National Laboratory (INL), and Sandia National Laboratories, provides an interactive tool to identify applicable standards based on project parameters including technology type, system characteristics, and jurisdiction [28].

To help stakeholders navigate this complex standards environment, The Energy Infrastructure Standards Search Tool, developed under the Securing Energy Infrastructure Executive Task Force, extends this guidance by helping stakeholders identify and map applicable standards to specific control system lifecycle phases [29].

3.4. Utility-Specific Policies

Individual utilities often develop their own technical requirements, interconnection agreements, and cybersecurity policies to address gaps in mandatory standards. Large IOUs may negotiate security requirements with manufacturers and establish comprehensive cybersecurity programs. However, resource constraints at some utilities, notably smaller municipal and cooperative utilities, can limit their ability to develop sophisticated policies. This creates variation in security posture based on utility size and resources rather than the actual risk profile of deployed assets. Two identical digital energy resource projects in different service territories may face different security and risk management hurdles based on utility capacity rather than technical necessity. The severity of this resource gap prompted DOE to launch the $250 million Rural and Municipal Utility Advanced Cybersecurity Grant program in 2023, recognizing that these not-for-profit utilities serve nearly one in six Americans often with limited cybersecurity resources [30].

4. GAP ANALYSIS

Despite the complex landscape of federal regulations, state actions, and voluntary standards, gaps remain between regulatory compliance and effective risk mitigation. The following outlines areas where utilities should be aware that compliance with current mandatory standards fails to provide adequate coverage or consistent protection.

4.1. Coverage Gaps Between Bulk & Distribution Systems

NERC CIP standards only protect the BES. Distribution-level assets and DERs fall under state jurisdiction or voluntary standards, as discussed in Section 3.1. This creates a regulatory gap where electric distribution systems, DERs, and grid-edge monitoring and control are primarily under state and utility jurisdiction, not subject to enforceable mandatory federal cybersecurity standards. In response, DOE and NARUC have issued voluntary Cybersecurity Baselines for electric distribution systems and DERs as resources for states and utilities that choose to adopt them [31]. The objective of these supporting frameworks is to encourage and support vulnerable, less standardized grid entities to apply risk-based security protections. State actions vary, and uptake is not uniform across jurisdictions; consequently, distribution-level digital energy infrastructures are not subject to uniform mandatory federal cybersecurity standards, resulting in inconsistent protection across jurisdictions.

4.2. Self-Attestation & Voluntary Compliance

Self-attestation creates a verification paradox in which equipment holds certifications yet may not perform securely in operational contexts. IEEE 1547-2018, the standard for DER interconnection and interoperability, does not include cybersecurity requirements for DERs [32]. IEEE 1547.3-2023 has since been published as a voluntary cybersecurity guideline; it is not a mandatory requirement [33]. NERC's analysis in their 2022 white paper “Cyber Security for DERs and DER Aggregators” concluded that despite various cybersecurity standards and guides existing today, no standards or test procedures for certification purposes provide a complete list of detailed auditable requirements, with some in-depth documents written for product types outside renewables and some renewable-focused documents lacking the mandatory language needed for certification [32]. Consequences of relying on voluntary standards are evident in NLR testing that found industry-standard-certified inverters failed 9 out of 10 test cases in cybersecurity evaluations, potentially leaving commercial systems vulnerable to eavesdropping, man-in-the-middle, and denial-of-service attacks [34].

The self-attestation challenge extends beyond equipment to organizational requirements. Utilities often accept vendor self-attestations of security practices without independent verification mechanisms, and some state cybersecurity requirements similarly rely on utility self-attestation without enforcement or audit capabilities. While some states require utilities to develop cybersecurity plans, requirements may lack specific, measurable targets (such as incident disclosure timeframes or patch management schedules), leaving utilities to define their own metrics based on varying risk tolerances and resource constraints. Beyond initial certification weaknesses, operational security risk changes over time as certifications may not account for configuration changes, delayed patching, integration with legacy systems, or commission errors, and potential lack of mandatory field verification or periodic recertification requirements to ensure certified equipment maintains security posture once operational.

4.3. Emerging Technologies & Supply-Chain Risks

Digital energy infrastructure increasingly incorporates technologies that outpace standard development cycles and introduce unfamiliar attack surfaces. According to the U.S. 2024 Energy Modernization Cybersecurity Implementation Plan, the energy sector’s exposure to remote cyber threats has grown as companies connect operational technology (OT) to the Internet to manage widespread systems [35]. **While increasing connectivity and digitalization cuts costs and boosts efficiency, many legacy systems were not built for secure online operation, creating new cybersecurity risks that**

threaten grid reliability.Error! Bookmark not defined. In theory, expansive virtualization increases the risk that if one system is hacked, others on the same platform could be affected. Similarly, cloud-based energy management tools give utilities flexibility and better access to data, but they also rely on outside providers. This creates new security concerns about who controls the data, how users are verified, the asset supply chain, and what happens if the cloud service is disrupted.

Industry experts describe a "race to the bottom" pricing environment in which inverters have become commoditized over the past five years, with vendors using default passwords such as "12345678" across entire product categories [36]. While DOE has provided cybersecurity procurement language frameworks since 2014, adoption remains voluntary and many organizations may continue to prioritize cost and delivery speed over security requirements in their request for proposals [37]. These practices have created systemic vulnerabilities, with Forescout researchers discovering 46 critical flaws across three top solar inverter manufacturers' web APIs, gateways, and inverters that could enable attackers to compromise or disrupt entire inverter fleets [38].

Technological advances intersect with supply chain vulnerabilities, increasing security risks. FERC has proposed directing NERC to develop new or modified reliability standards that require entities to "identify their current supply chain risks to their grid-related cybersecurity systems at specified intervals, assess and take steps to validate the accuracy of the information received from vendors during the procurement process, and document, track and respond to these risks to their systems" [39]. However, these standards focus on BES assets. The Department of Energy's January 2025 report on the BESS supply chain explicitly addresses risks posed by foreign-manufactured components and provides frameworks for assessing the current equipment already deployed [40].

4.4. Slow Evolution & Adoption of Industry Standards

Digital energy resources evolve rapidly, introducing new technologies and capabilities faster than safety standards can be written, adapted, or implemented. BESS illustrate this challenge with safety standards from which the industry can take lessons that can be applied to cybersecurity standards. Early deployments operated under generic requirements designed for other applications rather than code addressing the specific hazards of large-scale, stationary, grid-connected battery systems [41]. Standards developed for small portable consumer batteries were inappropriately applied to utility-scale installations with different risk profiles. BESS safety codes began to emerge only after multiple serious incidents prompted regulatory action, with 23 fires at South Korean energy storage facilities between June 2018 and January 2019 catalyzing significant changes to the codes and standards landscape [42].**Error! Bookmark not defined.** Safety standards are often developed reactively, with major incidents driving code changes only after facilities are already deployed and operating.

The consequences of this gap are illustrated by the McMicken Battery Energy Storage System explosion in Arizona on April 19, 2019, which occurred before NFPA 855's first edition was released later that year [43]. When firefighters opened the facility door after battery failure began, accumulated flammable gases exploded, injuring multiple responders. The facility's fire suppression system, which the manufacturer had acknowledged two years earlier was inadequate for cascading thermal runaway, could not prevent the disaster.**Error! Bookmark not defined.** Lessons from McMicken informed the 2020 and 2023 editions of NFPA 855, yet most states still operate under fire codes predating these updates. One investigation into this incident concluded that "many standards are now in place that were not at the time of the system's commissioning" [44]." The Fire Suppression Systems Association has stated that, although it supports new and alternative energy technologies, the use of older NFPA editions may put the public at risk. However, the common practice of multi-year adoption cycles perpetuates the exposure [45]. Rather than wait for major cybersecurity incidents to take place, encouraging both rapid development of critical standards and adoption of best practices for security before standards are approved can help mitigate the likelihood of major cyber events affecting reliability or safety.

Additionally, states adopt codes on vastly different timelines, creating gaps in requirements that leave utilities and communities at potential risk between when hazards are understood and when standards are written or become enforceable. Illustrative examples of this issue include:

- As of April 2021, eight states remained on the 2012 fire code cycle, 23 states on the 2015 cycle, 17 states on the 2018 cycle, and only California and New York had adopted the current 2021 cycle incorporating NFPA 855 [46].
- The DOE's 2024 strategic plan notes that states can be operating on up to three different editions of the International Fire Code simultaneously, with the most current edition potentially taking another two to six years to be adopted in most states [47].
- Washington State's early adoption of NFPA 855 (2023) and select 2024 International Fire Code provisions ahead of their formal code cycle illustrates both the urgency and uneven pace of safety code evolution, as jurisdictions attempt to bridge the gap between emerging battery technologies and lagging regulatory frameworks [48].
- State tracking of IEEE 1547-2018 adoption shows that, as of 2024, only seven states have completed adoption, while three remain incomplete, six are ongoing, and the remainder have either incomplete or utility-specific adoption [22].**Error! Bookmark not defined.**

While this gap analysis has focused on battery energy storage and fire safety codes as illustrative examples, the underlying challenge extends across all digital energy resources. The same pattern of technology outpacing standards, followed by multi-year delays in state adoption, can impact utilities integrating digital energy resources.

5. RECOMMENDATIONS

Utilities deploying digital energy technologies and connected grid assets face a critical challenge - compliance with applicable standards does not always guarantee operational security or resilience. As grid digitization accelerates faster than standards and regulation evolve, utilities and vendors must adopt a more deliberate, risk-informed approach to applying existing standards and augmenting them where gaps remain.

The following recommendations are intended to help utilities, vendors, and regulators close the gap between compliance with existing standards and effective cybersecurity and operational risk management for digital energy systems, particularly for distribution-level assets, grid communications, and emerging technologies that fall outside mandatory federal requirements.

5.1. Prioritize Adoption of Existing Standards Where Applicable

Where cybersecurity and safety standards already exist, utilities should adopt and align to those standards and require vendor conformance, rather than creating new requirements. Leveraging recognized standards reduces fragmentation across the vendor ecosystem, lowers compliance burden for suppliers serving multiple customers, and promotes consistency in implementation. Mandatory federal standards such as NERC CIP establish enforceable cybersecurity baselines for BES assets, while NERC O&P standards govern the reliability performance of certain IBRs. For distribution-level assets and DERs outside mandatory federal scope, utilities can align to existing voluntary frameworks, such as DOE’s Cybersecurity Capability Maturity Model (C2M2), the DOE Supply Chain Cybersecurity Principles, and the National Cyber-Informed Engineering (CIE) Strategy, which collectively support risk-based governance, engineering, and procurement decisions. Widely recognized consensus standards, including IEEE 1547-2018, NIST’s Cybersecurity Framework, ISA/IEC 62443 for industrial control systems, and UL standards for device-level security, provide established technical baselines that can be contractually enforced even where regulation does not mandate them.

Emphasizing existing standards brings industry attention to areas where standards are outdated or incomplete, supporting broader participation in standards bodies and helping ensure standards evolve alongside emerging technologies. Not all digital energy assets require the same level of protection. Utilities should categorize assets based on their potential operational impact, considering factors such as aggregated capacity, criticality to grid stability, and consequences of compromise or failure. Higher-risk assets warrant more stringent controls, including the adoption of voluntary standards that exceed minimum regulatory requirements. Lower-risk assets may be adequately protected through manufacturer guidance and basic security hygiene, provided utilities understand and accept the residual risk. The key is to match security investment to consequence when selecting which requirements to apply across different asset types.

5.2. Address Grid Communications & Emerging Technology Risks

A significant portion of cybersecurity risk in digital energy technology exists in grid communications and emerging technologies that fall outside mandatory federal cybersecurity standards. NERC CIP requirements focus on assets within defined electronic security perimeters and explicitly exclude communications infrastructure beyond those boundaries, including routers, modems, leased circuits, cloud-managed platforms, and third-party telecommunications services that carry critical operational data. These exclusions originated as practical accommodations when utilities relied on external communications providers outside federal jurisdiction. As grid operations have become increasingly interconnected, this approach has created persistent gaps affecting control-center communications, inter-facility data flows, and remote monitoring and control pathways that are mission-critical but not uniformly governed by enforceable standards [49]. Additionally, as utilities adopt cloud-based energy management and virtualized control systems, independent audits of identity management, encryption, and multi-tenancy isolation become increasingly critical.

Where standards do not yet fully apply, utilities and vendors must collaborate to adopt best practices that reflect operational risk. Communications and emerging technology security should be treated as integral to risk management by establishing interim expectations for authentication, encryption, monitoring, remote access, and data handling across organizational boundaries. Clear definition and communication of security assumptions and responsibilities among stakeholders reduces misalignment and supports consistent implementation. Based on the unique configurations and mix of technologies, vendors, and solution providers involved with individual projects, standardized approaches may not always be possible. Where standardization cannot provide appropriate coverage, customized, risk-based approaches should be adopted to secure digital energy technologies.

5.3. Move Beyond Self-Attestation Through Continuous Validation

Many standards applicable to digital energy systems rely on self-attestation or one-time certification, creating a structural gap between formal compliance and operational security. Certification often confirms that a requirement was met at a specific point in time but does not verify that security controls continue to function as systems are deployed, integrated, updated, and remotely managed. Evidence shows that this gap can leave utilities exposed even when systems meet recognized standards. Continuous validation addresses this gap by shifting assurance from documentation to evidence. Rather than treating certification as the endpoint, utilities can periodically validate that controls operate as intended in their deployed environment through recurring vulnerability assessments, configuration reviews, and functional testing that reflects operational conditions. Validation is particularly important for digital energy systems whose risk profiles change over time due to firmware updates, integration with utility networks, aggregation platforms, and cloud-based management tools.

Many digital energy assets operate outside mandatory cybersecurity oversight and are integrated incrementally through pilots, vendor-managed platforms, or third-party aggregators. In these environments, undocumented connections and unmanaged interfaces are common sources of exposure.

Maintaining accurate asset inventories, connectivity diagrams, and configuration baselines allows utilities to confirm that deployed systems match approved designs, detect unauthorized changes, and ensure that security expectations established during procurement and interconnection are actually implemented in the field. Inventory validation also supports lifecycle risk management by enabling utilities to track patch eligibility, end-of-support timelines, and evolving dependencies that may not be captured in initial certification or self-attestation.

Procurement and contracting represent a critical leverage point for enforcing continuous validation where regulation and standards fall short. As previously noted, many cybersecurity frameworks and procurement guidance documents are voluntary, yet they provide utilities with mechanisms to translate expectations into enforceable requirements. Contract terms can require vendors to support independent testing, disclose vulnerabilities within defined timeframes, maintain patch and support lifecycles, and provide updated documentation as systems evolve. Procurement and contracting language should explicitly define cybersecurity requirements, including vendor commitments to vulnerability disclosure, ongoing patch and support lifecycles, and alignment with recognized or emerging cybersecurity standards, even where formal certification programs do not yet exist. Utilities seeking practical guidance can reference Center for Securing Digital Energy Technologies (CSDET)'s Procurement, Contracting, and Supply Chain Risk Management Guidance, which outlines approaches for incorporating risk-based cybersecurity and supply-chain considerations into procurement and contracting processes [49].

5.4. Apply a Consequence-Based Approach

Standards establish minimum expectations, but they do not guarantee security or resilience. Overreliance on standards can create a false sense of assurance if risk is not evaluated in operational context, particularly for digital energy systems that vary widely in connectivity, autonomy, and consequence. Utilities can assess how failures or malicious manipulation of digital energy systems would affect grid stability, energy supply, safety, economic performance, environmental outcomes, and public trust through a consequence-driven approach. The framework outlined in the 2024 DOE BESS supply chain report leverages the Cyber-Informed Engineering (CIE) approach, to provide utilities with a consequence-driven framework to prioritize protections based on the real-world impact of misoperation or failure rather than uniform compliance across all assets [40].

Where standards or regulation do not yet apply, consequence scoring provides a rational basis for adopting interim controls using available best practices, research-based guidance, and cross-sector lessons learned rather than deferring action until mandates emerge. Additionally, organizations should regularly test backup systems and manual override capabilities to ensure operational continuity during cyber incidents.

5.5. Scale Implementation to Organizational Capacity

Small municipal utilities and cooperatives face different resource constraints than large investor-owned utilities. Recommendations must be practical for organizations with limited cybersecurity staff and budgets. These utilities should focus initial efforts on foundational controls that provide broad risk reduction, such as identifying which assets exist and where they connect to networks, implementing basic network segmentation, and establishing systematic patching approaches. The National Rural Electric Cooperative Association's Co-op Cyber Goals Program provides a structured framework of 20 actionable cybersecurity goals explicitly designed for cooperatives, with over 450 cooperatives participating as of the end of 2025 [51]. Additionally, small utilities benefit from cross-collaboration and established partnerships with other utilities of similar or larger scale. Cooperatives and municipal utilities, which typically fall outside PUC regulatory jurisdiction, can also engage State Energy Offices and state legislatures for partnerships, funding opportunities, and technical assistance on cybersecurity initiatives. This also includes collaboration with federal research laboratories, which excel in assessment and creation

of supporting frameworks. Capitalizing on free open-source tools and networked partnerships, rural/small utility service providers can extend capabilities beyond what internal resources alone could achieve.

Cross-utility collaboration ensures that lessons learned at scale inform practical, adoptable approaches across the sector. Larger utilities with greater resources should consider establishing dedicated OT security expertise separate from corporate enterprise cybersecurity, recognizing that OT environments have different requirements and threat models. These organizations are well-positioned to lead industry initiatives, develop practical implementation guidance for emerging standards, and contribute to sector-wide security improvements. Utilities vary significantly in staffing, budget, and technical depth, and implementation of these recommendations must reflect that reality. Scaling security efforts does not change risk, but it does shape how standards adoption, validation, and collaboration are applied in practice. Smaller municipal utilities and cooperatives should prioritize foundational controls that provide broad risk reduction, such as asset visibility, network segmentation, and systematic patch management. Structured frameworks like NRECA's Co-op Cyber Goals demonstrate how meaningful progress can be achieved with limited resources. Partnerships with stakeholders such as peer utilities, State Energy Offices, and national laboratories can extend capability beyond internal staff.

Additionally, utilities can engage independent cybersecurity firms and/or national labs to perform penetration tests and adversarial simulations on operational technology (OT) environments and grid-edge devices as well as periodically re-test devices under operational conditions to ensure security controls remain effective after updates or integration.

6. CONCLUSION

The U.S. digital energy ecosystem operates under a layered framework of federal mandates, state oversight, voluntary consensus standards, and utility-specific requirements. Together, these mechanisms establish an essential baseline for safety, reliability, and cybersecurity. They enable interoperability, support regulatory accountability, and provide common reference points for utilities, vendors, and regulators. Yet this baseline increasingly lags the reality of grid modernization. Rapid digitization, expanding grid communications, and the proliferation of distributed and inverter-based resources have shifted operational risk toward assets and interfaces that fall outside uniform, enforceable federal cybersecurity coverage.

Evidence shows that compliance does not consistently equate to risk reduction. Mandatory NERC CIP standards apply to a minority of grid assets, while the majority of digitally connected systems operate under voluntary, self-attested, or inconsistently enforced requirements. Empirical testing has demonstrated that certified devices can still fail basic cybersecurity evaluations, and real-world incidents such as exposed inverter fleets and delayed BESS safety code adoption illustrate how gaps between standards development, adoption, and enforcement translate into operational and public-safety consequences. These gaps are most acute at the distribution level and among smaller utilities with limited resources, but their effects can propagate across interconnected systems.

Closing this gap does not require abandoning existing standards or imposing uniform regulation across all assets. It requires a risk-informed application of the frameworks already in place. Utilities can treat standards as a foundation rather than a ceiling, applying consequence-based prioritization, continuous validation, and CIE to address uncovered communications paths, emerging technologies, and supply-chain dependencies. Procurement and contracting can provide utilities immediate leverage to translate expectations into enforceable controls, while independent assessment and operational testing help ensure that security measures perform as intended over time. This balanced, scalable approach allows utilities to improve security today while respecting jurisdictional boundaries and organizational capacity. By adopting existing standards where applicable, supplementing them with evidence-based interim controls, validating security claims in operational environments, and aligning protections with real-world consequences, utilities and regulators can steadily narrow the gap between regulatory compliance and actual grid resilience. This approach strengthens near-term risk management and provides

the empirical foundation needed for future standards and regulatory evolution, ensuring that digital energy innovation advances without outpacing security.

7. REFERENCES

[1] North American Electric Reliability Corporation (NERC), "2025 ERO Reliability Risk Priorities Report," 17 December 2025. [Online]. Available: https://www.nerc.com/globalassets/our-work/reports/white-papers/2025_risc_ero_priorities_report.pdf. [Accessed 7 February 2026].

[2] UL Solutions, "New Cybersecurity Threats to Renewable Energy Generation," UL Solutions, 6 February 2025. [Online]. Available: https://www.ul.com/insights/new-cybersecurity-threats-renewable-energy-generation.

[3] Forescout Research - Verdere Labs, "The Security Risks of Internet-Exposed Solar Power Systems," Forescout, 3 June 2025. [Online]. Available: https://www.forescout.com/blog/the-security-risks-of-internet-exposed-solar-power-systems/ .

[4] R. Lakshmanan, "Over 145,000 Industrial Control Systems Across 175 Countries Found Exposed Online," The Hacker News, 21 November 2024. [Online]. Available: https://thehackernews.com/2024/11/over-145000-industrial-control-systems.html .

[5] B. Toulas, "Over 130,000 solar energy monitoring systems exposed online," Bleeping Computer, 6 July 2023. [Online]. Available: https://www.bleepingcomputer.com/news/security/over-130-000-solar-energy-monitoring-systems-exposed-online/ .

[6] Littleton Electric Light and Water Departments , "LELWD Publicizes Case Study on Foreign Hackers Targeting U.S. Utilities," 14 March 2025. [Online]. Available: https://www.lelwd.com/wp-content/uploads/2025/03/LELWD-Publicizes-Case-Study-on-Foreign-Hackers-Targeting-US-Utilites.pdf .

[7] B. Sobczak, "First-of-a-kind U.S. grid cyberattack hit wind, solar," E&E News, 31 October 2019. [Online]. Available: https://www.eenews.net/articles/first-of-a-kind-u-s-grid-cyberattack-hit-wind-solar/.

[8] D. Phelan, "A Summary of State Regulators' Responsibilities Regarding Cybersecurity Issues," December 2014. [Online]. Available: https://pubs.naruc.org/pub/FA85B773-9EC1-54D6-C50E-8DD2A0D2D4EB.

[9] North American Electric Reliability Corporation (NERC), "Sanction Guidelines of the North American Electric Reliability Corporation (Appendix 4B)," 1 July 2014. [Online]. Available: https://www.nerc.com/globalassets/standards/resources/documents/appendix_4b_of_the_rules_of_procedure_sanction_guidelines.pdf.

[10] North American Electric Reliability Corporation (NERC), "Inverter-Based Resource Strategy," June 2022. [Online]. Available: https://www.nerc.com/comm/Documents/NERC_IBR_Strategy.pdf. [Accessed 27 October 2025].

[11] Federal Energy Regulatory Commission (FERC), "18 CFR Part 40 [Docket No. RM15-14-002; Order No. 829] Revised Critical Infrastructure Protection Reliability Standards," 21 July 2016. [Online]. Available: https://www.ferc.gov/sites/default/files/2020-04/E-8_1.pdf. [Accessed 27 October 2025].

[12] "18 CFR Part 40 [Docket No. RM17-13-000; Order No. 850] Supply Chain Risk Management Reliability Standards," 18 October 2018. [Online]. Available: https://www.ferc.gov/media/order-no-850. [Accessed 27 October 2025].

[13] Federal Energy Regulatory Comission (FERC), "FERC Order No. 2222: Fact Sheet," 28 September 2020. [Online]. Available: https://www.ferc.gov/media/ferc-order-no-2222-fact-sheet. [Accessed 27 October 2025].

[14] Federal Energy Regulatory Comission (FERC), "E-17-RD21-2-000," 18 March 2021. [Online]. Available: https://www.ferc.gov/media/e-17-rd21-2-000. [Accessed 27 October 2025].

[15] Federal Energy Regulatory Comission (FERC), "Incentives," FERC, 9 July 2023. [Online]. Available: https://www.ferc.gov/incentives. [Accessed 27 October 2025].

[16] Federal Energy Regulatory Comission (FERC), "FERC Takes Action to Enhance Reliability of the U.S. Electric Grid," 18 September 2025. [Online]. Available: https://www.ferc.gov/news-events/news/ferc-takes-action-enhance-reliability-us-electric-grid. [Accessed 27 October 2025].

[17] DOE Office of Cybersecurity, Energy Security, and Emergency Response (CESER), "Cybersecurity Capability Maturity Model (C2M2)," U.S. Department of Energy, 2022. [Online]. Available: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2. [Accessed 27 October 2025].

[18] "Distributed Energy Resource Cybersecurity Framework," National Laboratory of the Rockies, [Online]. Available: https://dercf.nrel.gov/. [Accessed 27 October 2025].

[19] DOE Office of Cybersecurity, Energy Security, and Emergency Response (CESER), "Supply Chain Cybersecurity Principles," U.S. Department of Energy, [Online]. Available: https://www.energy.gov/ceser/supply-chain-cybersecurity-principles. [Accessed 7 February 2026].

[20] DOE Office of Cybersecurity, Energy Security, and Emergency Response, "National Cyber-Informed Engineering Strategy," June 2022. [Online]. Available: https://www.energy.gov/sites/default/files/2022-06/FINAL%20DOE%20National%20CIE%20Strategy%20-%20June%202022_0.pdf. [Accessed 27 October 2025].

[21] U.S. Department of Energy and the National Association of Regulatory Utility Commissioners, "Cybersecurity Baselines for Electric Distribution Systems and DER," January 2025. [Online]. Available: https://www.energy.gov/sites/default/files/2025-01/Cybersecurity%20Baselines%20for%20Electric%20Distribution%20System%20Interim%20Implementation%20Guidance.pdf. [Accessed 27 October 2025].

[22] R. Walton, "Smart Inverter States: New Map Shows Progress of IEEE 1547-2018 Adoption," Microgrid Knowledge, 10 May 2024. [Online]. Available: https://www.microgridknowledge.com/design-engineering/article/55038946/smart-inverter-states-new-map-shows-progress-of-ieee-1547-2018-adoption. [Accessed 27 October 2025].

[23] D. Shea, "Cybersecurity and the Electric Grid | The State Role in Protecting Critical Infrastructure," National Conference of State Legislatures, 24 January 2020. [Online]. Available: https://www.ncsl.org/energy/cybersecurity-and-the-electric-grid-the-state-role-in-protecting-critical-infrastructure. [Accessed 27 October 2025].

[24] United States Government Accountability Office, "Electric Grid Cybersecurity: DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems," March 2021. [Online]. Available: https://www.gao.gov/assets/gao-21-81.pdf. [Accessed 27 October 2025].

[25] "Cybersecurity for Utility Regulators," National Association for Regualtory Utility Comissioners, [Online]. Available: https://www.naruc.org/core-sectors/critical-infrastructure-and-cybersecurity/cybersecurity-for-utility-regulators/. [Accessed 27 October 2025].

[26] National Association of Regulatory Utility Comissioners (NARUC, "Essential Guide to NARUC Cybersecurity Resources," [Online]. Available: https://pubs.naruc.org/pub/403C8E5A-99E0-B07E-7A13-6817D9CCFC95. [Accessed 27 October 2025].

[27] A. Colthorpe, "National Fire Protection Association releases NFPA 855 ESS safety standard, 2026 edition," Energy Storage News, 18 September 2025. [Online]. Available: https://www.energy-storage.news/national-fire-protection-association-releases-nfpa-855-ess-safety-standard-2026-edition/. [Accessed 27 October 2025].

[28] "DER Standards Library," OpenEI, [Online]. Available: https://apps.openei.org/der-cyber-standards/. [Accessed 27 October 2025].

[29] DOE Office of Cybersecurity, Energy Security, and Emergency Response (CESER), "Standards to Secure Energy Infrastructure," DOE CESER, [Online]. Available: https://energyicsstandards.inl.gov/. [Accessed 27 October 2025].

[30] M. Cox, "New Prize Supports Rural and Municipal Utilities in Strengthening Cybersecurity Posture," National Laboratory of the Rockies, 30 August 2023. [Online]. Available: https://www.nrel.gov/news/detail/program/2023/new-prize-supports-rural-and-municipal-utilities-in-strengthening-cybersecurity-posture. [Accessed 7 February 2026].

[31] DOE Office of Cybersecurity, ENergy Security, and Emergency Response (CESER) and the National Association of Regulatory Utility Comissioners (NARUC), "Cybersecurity Baselines for Electric Distribution Systems and DER," February 2024. [Online]. Available: https://www.energy.gov/sites/default/files/2025-01/NARUC_Cybersecurity-Baselines-Report%201.pdf. [Accessed 27 October 2025].

[32] North American Electric Reliability Corporation (NERC), "Cyber Security for Distributed Energy Resources and DER Aggregators," December 2022. [Online]. Available: https://www.nerc.com/comm/RSTC_Reliability_Guidelines/White_Paper_Cybersecurity_for%20DERs_and_DER_Aggregators.pdf. [Accessed 27 October 2025].

[33] Electric Power Research Institute (EPRI), "Status of IEEE P1547 Ongoing Revision: 2025 Update," 3 September 2025. [Online]. Available: https://www.epri.com/research/products/000000003002033780. [Accessed 27 October 2025].

[34] W. Hupp, D. Saleem, J. T. Peterson and K. Boyce, "Cybersecurity Certification Recommendations for Interconnected Grid Edge Devices and Inverter Based Resources," November 2021. [Online]. Available: https://docs.nlr.gov/docs/fy22osti/80581.pdf. [Accessed 7 February 2026].

[35] The White House, "Energy Modernization Cybersecurity Implementation Plan," December 2024. [Online]. Available: https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/12/Energy-Modernization-Cybersecurity-Implementation-Plan.pdf. [Accessed 27 October 2025].

[36] M. Nadeau, "Why cyber attackers are targeting your solar energy systems — and how to stop them," CSO Online, 3 March 2025. [Online]. Available: https://www.csoonline.com/article/3829736/why-attackers-target-companys-solar-energy-system-and-how-to-stop-them.html. [Accessed 27 October 2025].

[37] Energy Sector Control Systems Working Group (ESCSWG), "Cybersecurity Procurement Language for Energy Delivery Systems," April 2014. [Online]. Available: https://www.energy.gov/ceser/articles/cybersecurity-procurement-language-energy-delivery-april-2014. [Accessed 27 October 2025].

[38] S. Dashevskyi, F. L. Spina and D. d. Santos, "SUN:DOWN Destabilizing the Grid via Orchestrated Exploitation of Solar Power Systems," 27 March 2025. [Online]. Available: https://www.forescout.com/resources/sun-down-research-report/. [Accessed 27 October 2025].

[39] Federal Energy Regulatory Comission (FERC), "FERC Acts to Improve Reliability by Closing Supply Chain Cyber Risk Management Gaps," FERC, 19 September 2024. [Online]. Available: https://ferc.gov/news-events/news/ferc-acts-improve-reliability-closing-supply-chain-cyber-risk-management-gaps#:~:text=Dockets:%20RM24%2D4;%20RM24,assets%2C%20or%20%E2%80%9CPCAs.%E2%80%9D. [Accessed 7 February 2026].

[40] DOE Office of Cybersecurtiy, Energy Security, and Emergency Response (CESER), "Battery Energy Storage Systems Report," 1 November 2024. [Online]. Available: https://www.energy.gov/sites/default/files/2025-01/BESSIE_supply-chain-battery-report_111124_OPENRELEASE_SJ_1.pdf. [Accessed 27 October 2025].

[41] Electric Power Research Institute (EPRI), "The Evolution of Battery Energy Storage Safety Codes and Standards," 26 November 2023. [Online]. Available: https://www.epri.com/research/products/000000003002028521. [Accessed 27 October 2025].

[42] A. Colthorpe, "Korea's ESS fires: Batteries not to blame but industry takes hit anyway," Energy Storage News, 19 June 2019. [Online]. Available: https://www.energy-storage.news/koreas-ess-fires-batteries-not-to-blame-but-industry-takes-hit-anyway/. [Accessed 7 February 2026].

[43] G. Burdick, "APS says runaway thermal event caused 2019 battery explosion, outlines 4 steps to avoid a repeat," Utility Dive, 29 July 2020. [Online]. Available: https://www.utilitydive.com/news/aps-says-runaway-thermal-event-caused-2019-battery-explosion-outlines-4-st/582475/. [Accessed 27 October 2025].

[44] A. Colthorpe, "Arizona battery fire's lessons can be learned by industry to prevent further incidents, DNV GL says," Energy Storage News, 29 July 2020. [Online]. Available: https://www.energy-storage.news/arizona-battery-fires-lessons-can-be-learned-by-industry-to-prevent-further-incidents-dnv-gl-says/.

[45] B. Stinner, "The Adoption and Use of NFPA 855 in States and Local Communities," Fire Surpression Systems Association, 20 September 2022. [Online]. Available: https://www.fssa.net/index.php?option=com_dailyplanetblog&view=entry&year=2022&month=09&day=19&id=10:the-adoption-and-use-of-nfpa-855-in-states-and-local-communities. [Accessed 27 October 2025].

[46] J. Sanchez, "Fire Codes and NFPA 855 for Energy Storage Systems," Mayfield Renewables, 16 December 2021. [Online]. Available: https://www.mayfield.energy/technical-articles/fire-codes-and-nfpa-855-for-energy-storage-systems/. [Accessed 27 October 2025].

[47] DOE Office of Electricity, "Energy Storage Safety Strategic Plan," April 2024. [Online]. Available: https://www.energy.gov/sites/default/files/2024-05/EED_2827_FIG_SafetyStrategy%20240505v2.pdf. [Accessed 27 October 2025].

[48] K. Grove, "Pre-Implementation of NFPA 855 (2023) and 2024 IFC Provisions Related to Energy Storage Systems, Lithium-Ion Batteries, and Micromobility Devices," Washington State Fire Marshals, 5 July 2023. [Online]. Available: https://www.wsafm.com/news/13223796. [Accessed 7 February 2026].

[49] Idaho National Laboratory, "Securing Grid Communications," Idaho National Laboratory, INL/RPT-25-89588, Idaho Falls, ID, 2026.

[50] E. M. Stewart, R. V. Stolworthy, S. Gribbin, T. L. Briggs and M. J. Culler, "Securing Digital Energy Infrastructure: Procurement, Contracting, and Supply Chain Risk Management Guidance," October 2024. [Online]. Available: https://www.osti.gov/servlets/purl/2473239/. [Accessed 27 October 2025].

[51] National Rural Electric Cooperative Association, "Co-op Cyber Goals Program: Third Year In Review," NRECA, January 2026. [Online]. Available: https://www.cooperative.com/programs-services/bts/rc3/cyber-goals/Documents/Advisory-Co-op-Cyber-Goals-Year-3-Review-Jan-2026.pdf. [Accessed 7 February 2026].