WHITE PAPER

Securing Grid Modernization: Cybersecurity Considerations and Recommendations for Advanced Distributed Energy Resource Integration Under District of Columbia Formal Case No. 1050 (Interconnection Reform)

A Strategic Framework for Secure and Resilient Grid Modernization in the District of Columbia

Prepared to Support Stakeholder Engagement for the District of Columbia Formal Case No. 1050 Technical Conference

August 2026

About DOEE

The District Department of Energy and Environment (DOEE) leads the District of Columbia's efforts to advance environmental stewardship, energy resilience, and sustainable communities. As part of these efforts, DOEE's Clean Energy Division is supporting the modernization of the District's electric distribution system through the implementation of IEEE 1547-2018, the cybersecurity guidance of IEEE 1547.3-2023, advanced distributed energy resource (DER) integration, advanced inverter deployment, and the ongoing Formal Case No. 1050 (FC1050) Interconnection Reform proceeding.

This white paper provides technical guidance to support stakeholder engagement on the cybersecurity, interoperability, and operational governance considerations associated with integrating advanced DER technologies into a modern electric distribution system. As DER adoption and digital connectivity continue to expand, cybersecurity has become a foundational component of grid modernization, requiring coordinated technical, regulatory, and operational approaches to protect critical infrastructure while enabling the reliable and interoperable integration of inverter-based resources.

Drawing upon the principles and recommendations of IEEE 1547-2018 and IEEE 1547.3-2023, this white paper presents cybersecurity considerations and best practices that support the objectives of FC1050 by promoting secure, resilient, and interoperable DER integration. It is intended to inform regulators, utilities, policymakers, technology providers, and other stakeholders as they collaborate to develop a modern electric distribution system that is resilient to evolving cyber threats while accelerating the District's clean energy and grid modernization goals.

Contents

Cybersecurity Considerations for Advanced DER Integration Under Formal Case 1050 (Interconnection Reform)

Author: **Laura A. Ward, Ph.D.** (U.S. Department of Energy (DOE) Energy Innovator Fellow, hosted by DOEE)

Reviewed and Approved by: **Thomas Bartholomew**, Associate Director, Clean Energy Division, DOEE

*DOEE gratefully acknowledges the stakeholders from **FORMAL CASE NO. 1050 TECHNICAL CONFERENCE**, reviewers, and technical advisors who contributed their expertise to this white paper, and the DOEE Clean Energy Division for supporting its preparation and publication.*

EXECUTIVE SUMMARY

The electric power sector is undergoing a fundamental transformation driven by the rapid deployment of distributed energy resources (DERs), advanced power electronics, digital communications, and increasingly intelligent distribution system operations. Historically, DER interconnection processes have focused on evaluating electrical performance characteristics, thermal loading, voltage regulation, protection coordination, hosting capacity, fault current contributions, and power quality, to ensure safe and reliable integration of customer-owned generation. These engineering assessments remain essential, but the evolution of advanced inverter-based resources, battery energy storage systems (BESS), microgrids, electric vehicles, resilience hubs, virtual power plants (VPPs), and Distributed Energy Resource Management Systems (DERMS) is fundamentally changing the role of DERs within the electric grid. DERs are becoming interconnected cyber-physical resources that exchange operational data, respond to utility control signals, and increasingly contribute to real-time distribution system operations.

IEEE 1547-2018 [1] defines what a DER can technically do, its grid-support functions, monitoring, configuration, and information exchange, but is explicit about what it does not do: Clause 10.9 states that the standard does not mandate cybersecurity requirements at the DER interface, and Annex D.4 places DER physical security and the networks connecting a DER to remote managing entities outside the standard's scope. IEEE 1547.3-2023 [2], published as the designated cybersecurity companion guide, fills that gap, organized around the NIST Cybersecurity Framework's [3] Identify, Protect, Detect, Respond, and Recover structure and six technical categories: Risk Assessment, Network Engineering, Access Control, Data Security, Security Management, and Coping With and Recovering From Security Events.

This white paper presents a strategic framework, grounded in that standards structure, for evaluating cybersecurity, interoperability, operational governance, and DERMS readiness as DER penetration increases in the District of Columbia. It does not propose new regulatory requirements or modify Formal Case No. 1050's current interconnection procedures; it identifies emerging technical, operational, and governance considerations to support stakeholder engagement, and it grounds those considerations in verified current facts: the active status of Formal Case No. 1050 (most recently Order No. 22745, November 2025) [4], the District's 15%-local-solar-by-2041 target under the Local Solar Expansion Act of 2022 [5], DOEE's own July 2026 distributed battery storage request for information [6], and documented, real-world DER cybersecurity incidents [7] rather than hypothetical risk alone.

The framework adds three elements not present in earlier drafts of this discussion paper: first, explicit treatment of Zero Trust Architecture, Secure-by-Design principles [8], Defense in Depth, secure boot, and API security as named organizing frameworks, alongside the access-control, segmentation, and telemetry-integrity guidance already established; second, a documented case study, Forescout Vedere Labs' March 2025 "SUN:DOWN" research [7] disclosing 46 vulnerabilities across three leading solar inverter manufacturers, grounding the paper's risk discussion in verified, current evidence rather than hypothetical language alone; and third, structured reference tables (a standards crosswalk, a nine-role stakeholder responsibility matrix, a risk matrix, and a trust-zone architecture table) that make the standard's structure usable by a non-specialist regulatory audience without requiring separate consultation of the full IEEE 1547.3-2023 text.

Ultimately, this white paper provides a strategic foundation for future discussions among utilities, regulators, policymakers, technology providers, equipment manufacturers, aggregators, and other stakeholders regarding the governance of secure DER integration, so that accelerating DER deployment

strengthens, rather than compromises, the reliability, resilience, operational visibility, and security of the District's critical energy infrastructure.

1. INTRODUCTION

The modernization of DER interconnection policy presents an opportunity to address not only traditional electrical system impacts but also the operational, interoperability, and cybersecurity considerations associated with increasingly digitalized distribution networks. Historically, DER interconnection reviews have focused on thermal loading, voltage regulation, protection coordination, hosting capacity, fault current contributions, and power quality. These assessments remain essential, but the rapid deployment of advanced inverter-based resources, BESS, microgrids, electric vehicle infrastructure, and VPPs is transforming DERs from passive generation assets into actively managed cyber-physical components of the electric grid.

Under IEEE 1547-2018, DERs are equipped with advanced grid-support functions and interoperability capabilities enabling communication and coordination with utility operational technology (OT) environments, SCADA systems, DERMS, ADMS, telemetry platforms, and other grid operational architectures. Interconnection frameworks are therefore becoming gateways not only for power flow integration but also for operational data exchange, remote visibility, monitoring, control, and system coordination. IEEE 1547-2018 is not intended to function as a comprehensive cybersecurity framework; as operational connectivity expands, IEEE 1547.3-2023 provides the complementary cybersecurity governance addressing industrial control system security, network segmentation, access control, asset management, secure communications, and cyber-physical risk management. IEC 62443 provides a widely recognized framework for securing industrial automation and OT environments and offers valuable guidance for DERMS-enabled distribution system operations.

This paper's scope note applies throughout: Formal Case No. 1050 primarily addresses interconnection modernization, technical screening, queue management, advanced inverter implementation, and export controls. The cybersecurity, operational technology, telemetry governance, DERMS integration, supply-chain security, and cyber-physical risk management considerations discussed in this paper extend beyond that traditional interconnection scope and are intended to support future stakeholder engagement and long-term grid modernization planning, not to prescribe requirements within the current proceeding. This note is stated once, here, and applies to every section that follows; it is not repeated at length elsewhere in this document.

1.1 PURPOSE AND SCOPE

The purpose of this paper is to examine emerging cybersecurity, interoperability, DERMS readiness, and operational governance considerations associated with advanced DER integration under IEEE 1547-2018, and to evaluate how increasing DER deployment may influence future utility operations, communications architectures, telemetry requirements, operational visibility, and cyber-physical system management. The paper is a discussion framework supporting stakeholder engagement; it does not establish regulatory requirements, technical standards, or implementation obligations.

1.2 WHY THIS DISCUSSION MATTERS

Advanced inverter-based resources are increasingly capable of providing communications, telemetry, monitoring, export management, grid-support functions, and interoperability capabilities that enable interaction with utility operational environments. Future grid modernization therefore requires consideration of both electrical integration and cyber-physical operational integration, an increasing

convergence of energy systems, communications systems, OT environments, and distributed control architectures that create new opportunities and new governance challenges for utilities, regulators, DER owners, aggregators, and technology providers.

1.3 RELATIONSHIP TO IEEE 1547-2018 IMPLEMENTATION AND FORMAL CASE NO. 1050

Although Formal Case No. 1050 is primarily focused on interconnection modernization, implementation of IEEE 1547-2018 introduces broader questions regarding communications interoperability, operational visibility, telemetry architecture, and future utility operational readiness. Related proceedings, including Formal Case No. 1163 on future microgrid policy [9], intersect directly with this paper's discussion of resilience hubs and grid-forming inverters and should be read alongside it.

1.4 IMPORTANT CONTEXT AND LIMITATIONS

Many of the cybersecurity, operational technology, telemetry governance, DERMS integration, supply-chain security, and cyber-physical risk management considerations discussed throughout this paper extend beyond traditional interconnection requirements and may be more appropriately addressed through future grid modernization initiatives, utility operational planning, DERMS implementation efforts, resilience planning, and related stakeholder processes, consistent with the scope note in Section 1. The observations and discussion questions in this paper should not be interpreted as proposed cybersecurity requirements for adoption within Formal Case No. 1050.

2. IEEE 1547-2018 AND THE EVOLUTION OF DER INTERCONNECTION

IEEE 1547-2018's [1] Clauses 4 through 9 govern general interconnection technical specifications, reactive power and voltage control, response to abnormal grid conditions, power quality, islanding, and behavior on secondary and spot network systems, and remain essential to safe and reliable electric service. Clause 10, "Interoperability, information exchange, information models, and protocols," is where the standard moves beyond electrical performance to define how a DER communicates, is monitored, and is configured, and is the technical basis for the remainder of this paper.

2.1 FROM ELECTRICAL INTERCONNECTION TO CYBER-PHYSICAL INTEGRATION

Clause 10.1 requires a DER to have a local DER communication interface supporting the information exchange requirements for every function it supports; the Area EPS operator (the utility) decides whether to rely on that interface alone or deploy a broader communication system around it. Clause 10.2 organizes exchangeable information into four categories: nameplate (read-only), configuration (read or write), monitoring (read-only), and management (read or write). This four-category structure is the standard's own answer to a cybersecurity-relevant question: which data streams are read-only telemetry and which are writable control channels that, if compromised, could change DER behavior.

2.2 ADVANCED INVERTERS AND INTEROPERABILITY

Clause 5.3 requires voltage regulation through one of four mutually exclusive reactive power modes, defaulting to constant power factor at unity unless the utility actively enables Volt-VAR or another mode. Clause 5.4 defines the companion Volt-Watt function, required only for Category B DER and disabled by default. Clause 6.5 governs frequency ride-through and tripping (OF1, OF2, UF1, UF2), with thresholds set by the utility in coordination with the regional reliability coordinator. Clause 10.7 requires a DER to

support at least one of three eligible protocols, IEEE 2030.5 (SEP2) [10], IEEE 1815 (DNP3) [11], or SunSpec Modbus; Clause 10.8 clarifies that communication performance requirements apply only to the DER's own interface, not the broader network connecting it to the utility.

2.3 DERMS, ADMS, AND UTILITY OPERATIONS

DERMS and ADMS platforms are not defined or required by IEEE 1547-2018; they are utility-operated platforms built on the interoperability foundation the standard provides. The operational questions that matter most, who holds command authority, who owns telemetry, how data quality is validated, and who is accountable for a given action, are addressed by IEEE 1547.3-2023's Access Control, Data Security, and stakeholder-role provisions (Section 2.8), not by IEEE 1547-2018 itself.

2.4 WHY IEEE 1547-2018 IS NOT A CYBERSECURITY STANDARD

Clause 10.9 states explicitly that IEEE 1547-2018 does not mandate cybersecurity requirements at the DER interface, treating such requirements as a matter for mutual agreement and applicable jurisdictional regulation, and directs readers to Annex D.4, which places DER physical security, front-panel security, and the networks connecting DER to remote managing entities outside the standard's scope. This is a deliberate scope boundary, not an oversight, and is the reason IEEE published IEEE 1547.3-2023 as a dedicated companion guide.

2.5 IEEE 1547.3-2023: PURPOSE AND STRUCTURE

IEEE 1547.3-2023 [2], approved June 5, 2023 and published December 11, 2023 as a full revision of IEEE 1547.3-2007, is IEEE's designated cybersecurity guide for DER interconnected with electric power systems, positioned as a complement to, not a replacement for, the ISO/IEC 27000 series, IEC 62443 [12], IEC 62351 [13], and the NIST frameworks [3, 14]. It adopts the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover) [3] as its organizing principle and maps its recommendations to specific NIST CSF subcategories. The companion Application Guide, IEEE 1547.2 [15], provides additional technical background on IEEE 1547-2018 itself and should be consulted alongside 1547.3-2023 for implementation context.

2.6 THE SIX TECHNICAL RECOMMENDATION CATEGORIES

IEEE 1547.3-2023 Clause 5 organizes its technical guidance into six categories, summarized in Table 1 together with where each is addressed in this framework. Each category carries a two-tier recommendation structure, a base tier of low-cost, high-impact recommendations expected at every installation, and an enhanced tier for higher-security-context deployments, allowing cybersecurity expectations to scale with DER size or criticality rather than imposing uniform requirements on a 5-kW residential system and a 5 MW aggregated portfolio alike.

Table 1. *IEEE 1547.3-2023 six-category structure mapped to this framework's governance sections.*

Category (IEEE 1547.3-2023 Clause 5)	Focus	Where Addressed in This Framework
Risk Assessment (RA)	Cross-organizational risk assessment spanning DER owner, integrator, aggregator, and utility	Section 3 (risk categories); Section 4.5 (ownership split)
Network Engineering (NE)	Segmentation and security boundaries between DER, aggregator, and utility OT	Section 5.2 (segmentation and trust boundaries)
Access Control (AC)	Identity, credential management, least privilege, logged remote access	Section 5.3 (authentication, identity, Zero Trust)
Data Security (DS)	Protection of data, firmware, and settings at rest and in transit	Section 5.4 (inverter settings, firmware, secure boot)
Security Management (SM)	Asset inventory and classification by criticality	Section 5.5 (logging, monitoring, auditability)
Coping With and Recovering From Security Events	Incident response roles, reporting, forensic analysis	Section 5.6 (incident reporting and response)

2.7 TESTING AND COMMISSIONING FOR CYBERSECURITY

IEEE 1547.3-2023 Clause 6 treats cybersecurity verification as a distinct lifecycle activity, running alongside, not folded into, the interconnection conformance testing defined in IEEE 1547.1-2020 [16]. Advanced-inverter interconnection testing and DER cybersecurity testing are related but procedurally separate activities; a future District framework should not assume that clearing the former satisfies the latter. Device-level certification standards, including UL 1741 [17] (interconnection and, in its Supplement SA form, advanced inverter functionality) and the anticipated UL 2941 [18] (DER-specific cybersecurity certification, currently in development), complement this lifecycle distinction at the manufacturer level.

2.8 DERMS, AGGREGATOR, AND OPERATIONAL RESILIENCE GOVERNANCE

IEEE 1547.3-2023 Annex F assigns cybersecurity responsibility across eleven defined stakeholder roles, summarized in Table 2, rather than treating DERMS and aggregator governance as a single undifferentiated category. Command authority, telemetry ownership, override authority during abnormal conditions, and cybersecurity responsibility allocation are all mapped to specific roles under this structure.

Table 2. *Stakeholder responsibility matrix based on IEEE 1547.3-2023 Annex F's nine defined roles.*

Role (IEEE 1547.3-2023 Annex F)	Primary Accountability	Cybersecurity Responsibility	Command / Override Authority
DER manufacturer	Device design and firmware	Secure-by-design engineering, vulnerability disclosure, SBOM	None
Integrator / installer	Commissioning	Secure configuration at installation, credential provisioning	None post-commissioning
Testing entity	Conformance verification	Cybersecurity test execution distinct from IEEE 1547.1 conformance testing	None
DER user (facility owner)	Asset ownership	Physical security, authorized access, prompt patching	Local operational control
DER user (utility operator)	Grid operations	OT segmentation, authenticated interfaces, monitoring	Grid-support settings within utility-approved bounds
DER user (aggregator)	Portfolio coordination	Aggregator platform security, contractual cybersecurity terms	Dispatch within contracted parameters

Facility ICT configuration developer	Communications setup	Secure protocol implementation, certificate issuance	None
Security managers	Governance oversight	Policy, incident response coordination, audit	Escalation and isolation authority
Maintenance personnel	Ongoing upkeep	Logged, authorized maintenance access	None outside authorized work orders
Operator (coping action)	Real-time event response	Immediate containment during an active event	Emergency isolation authority
Operator (recovery/analysis)	Post-event restoration	Forensic analysis, root-cause reporting, restoration verification	Restoration authorization

Operational resilience, fail-safe operating modes, communications-loss behavior, autonomous fallback, intentional islanding protections, and black-start coordination, sits within this same governance structure and is especially relevant for resilience hubs, advanced microgrids, and grid-forming inverter deployments.

2.9 THE LAYERED STANDARDS FRAMEWORK

IEEE 1547-2018 and IEEE 1547.3-2023 are the interconnection and DER-cybersecurity anchors, but both reference a broader standards landscape. IEEE 1547.3-2023 Annex D catalogs adjacent frameworks: the ISO/IEC 27000 series, the NIST Cybersecurity Framework [3], ISO 31000/22301, NISTIR 7628, the IEC 62443 series [12], IEC 62351 [13], NERC CIP for grid-reliability governance lessons [19] (including CIP-003's security management controls for low-impact BES Cyber Systems, increasingly relevant as aggregated DER capacity grows), and device-level standards including IEEE 1686 (cybersecurity capabilities of substation intelligent electronic devices) and IEEE C37.240 (cybersecurity for power system protection and control). Annex B catalogs the DER communication protocols already contemplated within the 1547 family: IEEE 1815 (DNP3) [11], IEC 61850 [20], IEEE 2030.5 [10], and SunSpec Modbus. DOE CESER [21] and NARUC have developed cybersecurity baselines for electric distribution systems and DERs aimed at state commissions, utilities, DER operators, and aggregators [22], and CISA's Cross-Sector Cybersecurity Performance Goals [23], together with CISA's Secure by Design pledge program [8], provide baseline practices applicable to critical infrastructure entities generally, including DER manufacturers (Section 5.9).

3. CYBER-PHYSICAL RISK MANAGEMENT CONSIDERATIONS

As DERs become increasingly interconnected through communications networks, telemetry platforms, advanced inverter functionality, DERMS architectures, aggregators, and cloud-based operational systems, cybersecurity events may create direct consequences for electric system operations, distinct from traditional IT environments where the consequences of a breach are primarily informational.

3.1 UNAUTHORIZED DER DISCONNECTION EVENTS

As DER penetration increases, coordinated disconnection of large numbers of distributed resources could affect feeder loading, voltage profiles, power quality, and system operations. While individual DER systems typically represent small amounts of capacity, aggregated impacts may become significant as deployment levels increase.

3.2 COORDINATED INVERTER MANIPULATION AND SETTINGS CHANGES

Advanced inverters increasingly support configurable grid-support functions such as Volt-VAR control, Volt-Watt control, frequency-watt response, ride-through settings, export management logic, and reactive power support. Unauthorized modification of these settings could alter expected DER behavior during abnormal grid conditions, as documented in the case study in Section 3.8.

3.3 FALSE TELEMETRY INJECTION AND DATA INTEGRITY RISKS

Future DERMS-enabled environments may rely on telemetry data to support operational visibility, forecasting, situational awareness, export management, and distributed resource coordination. Inaccurate, manipulated, delayed, or compromised telemetry could affect operational decision-making and reduce confidence in system visibility.

3.4 DERMS COMMAND PATHWAY COMPROMISE

DERMS platforms may eventually coordinate large numbers of distributed resources across multiple feeders. As coordination capabilities expand, the integrity, authenticity, and accountability of operational commands become increasingly important, and command authority, authentication mechanisms, operational approvals, and auditability requirements must be managed within DERMS-enabled operating environments.

3.5 COMMUNICATIONS DISRUPTION AND OPERATIONAL VISIBILITY LOSS

Communications disruptions may affect operational visibility, situational awareness, telemetry performance, and distributed resource coordination. Operational resilience planning benefits from consideration of communications failures, degraded operating modes, fallback strategies, and continuity of operations procedures.

3.6 SUPPLY CHAIN AND VENDOR RISKS

The increasing deployment of advanced inverters, communications gateways, telemetry systems, DERMS platforms, cloud-based services, and third-party operational technologies introduces supply-chain cybersecurity considerations: vendor lifecycle management, firmware integrity, software update validation, vulnerability disclosure processes, Software Bill of Materials (SBOM) transparency, and secure development practices, addressed further in Section 5.9.

3.7 RELIABILITY, RESILIENCE, AND ENERGY ASSURANCE IMPACTS

Cybersecurity considerations associated with DER integration ultimately extend beyond information technology concerns and may influence broader reliability, resilience, and energy assurance objectives as the District advances community solar, battery storage, resilience hubs, microgrids, vehicle-to-grid technologies, and future VPP architectures.

3.8 DOCUMENTED REAL-WORLD PRECEDENT: THE SUN: DOWN DISCLOSURES

The risk categories above are not solely hypothetical. In March 2025, Forescout's Vedere Labs published "SUN:DOWN: Destabilizing the Grid via Orchestrated Exploitation of Solar Power Systems" [7], disclosing

46 new vulnerabilities across three of the world's leading solar inverter vendors (Sungrow, Growatt, and SMA), including remote code execution, authentication bypass, and cloud-platform account takeover vulnerabilities that would have allowed an attacker to switch inverters on or off or manipulate their output settings. The research found that 80% of solar power system vulnerabilities disclosed over the prior three years were rated high or critical severity, with 30% receiving the maximum possible CVSS score. Separately, reporting in 2026 documented undisclosed communication devices found in certain imported solar inverters, underscoring the supply-chain dimension of Section 3.6. This precedent directly substantiates the settings-manipulation risk described in Section 3.2 and the supply-chain risk described in Section 3.6, and demonstrates that DER cybersecurity governance addresses a documented, current threat, not only a prospective one.

Table 3. *Qualitative risk matrix for the categories in Section 3, informed by the documented precedent in Section 3.8.*

Risk Category (Section 3)	Likelihood	Impact	Primary Mitigation Layer
Unauthorized DER disconnection (3.1)	Medium	Medium-High (aggregate)	Access control, network segmentation
Coordinated inverter settings manipulation (3.2)	Medium	High	Settings governance, secure firmware, secure boot
False telemetry injection (3.3)	Medium	Medium-High	Data integrity validation, anomaly detection
DERMS command pathway compromise (3.4)	Low-Medium	High	Zero Trust access, API security, segmentation
Communications disruption / visibility loss (3.5)	Medium-High	Medium	Fail-safe modes, autonomous fallback
Supply chain and vendor risk (3.6)	Medium-High	High	SBOM, secure-by-design procurement, vendor risk management
Reliability / resilience / energy assurance impact (3.7)	Low (today), rising	High	Defense in depth across all layers

4. REGULATORY CONTEXT FOR DISTRICT OF COLUMBIA INTERCONNECTION MODERNIZATION

4.1 OVERVIEW OF FORMAL CASE NO. 1050

Formal Case No. 1050 [4], the Public Service Commission of the District of Columbia's investigation into the implementation of interconnection standards in the District, is an active proceeding. Its most recent substantive order, Order No. 22745 (November 2025), established a Temporary Conditional Interconnection Program addressing DER projects in Pepco's queue as of October 31, 2025, and directed Pepco to file a quarterly equipment availability and procurement plan covering meters, communications hardware, relay protection equipment, and telemetry devices beginning January 1, 2026 [24]. The proceeding has focused on improving interconnection processes, enhancing transparency, reducing unnecessary barriers to DER deployment, supporting advanced inverter implementation, and evaluating approaches for accommodating increasing levels of distributed generation.

4.2 ADVANCED INVERTER IMPLEMENTATION CONSIDERATIONS

Advanced inverters provide capabilities extending well beyond traditional power conversion, including Volt-VAR control, Volt-Watt control, frequency response, reactive power management, ride-through, export management, telemetry services, and communications interoperability. Widespread deployment

introduces additional considerations involving interoperability validation, settings governance, communications architectures, telemetry performance, operational visibility, and long-term lifecycle management.

4.3 DERMS READINESS AND FUTURE UTILITY OPERATIONS

Increasing DER deployment is driving utilities to evaluate DERMS as a means of improving operational visibility and coordination. Future DERMS-enabled environments may involve interactions among utility OT systems, customer-owned DER assets, aggregators, advanced inverters, telemetry systems, communications networks, and third-party service providers, and DERMS readiness should be viewed as a component of broader grid modernization planning, not solely a technology implementation issue.

4.4 SCOPE OF INTERCONNECTION PROCEEDINGS VERSUS UTILITY OPERATIONAL GOVERNANCE

As stated in Section 1, cybersecurity, operational technology, telemetry governance, DERMS integration, supply-chain security, and cyber-physical risk management considerations discussed throughout this paper extend beyond the traditional scope of Formal Case No. 1050 and are intended to identify emerging considerations for future grid modernization initiatives, not to prescribe requirements within the current proceeding.

4.5 UTILITY-OWNED VERSUS CUSTOMER-OWNED DER CYBERSECURITY RESPONSIBILITY

Mapping the stakeholder roles in Table 2 onto the District's current structure clarifies a distinction the interconnection process does not currently make explicit. Pepco's OT-side responsibilities, SCADA and DERMS platform security, network segmentation, and authenticated command pathways, correspond to the "DER user (utility operator)" role. Customer and aggregator-side responsibilities, device security, authorized access, and (for aggregators) platform and contractual cybersecurity terms, correspond to the "DER user (facility owner)" and "DER user (aggregator)" roles. Under current District interconnection procedures, this division of responsibility is implicit rather than documented; a future framework would benefit from stating it explicitly, consistent with IEEE 1547.3-2023 Annex F, so that neither the utility nor the customer/aggregator side operates under an assumption that the other bears primary responsibility for a given control.

4.6 RELEVANCE OF FERC ORDER 2222 TO AGGREGATOR GOVERNANCE

FERC Order 2222 [25] (September 2020) requires regional transmission organizations, including PJM, the wholesale market operator within whose footprint the District sits, to allow DER aggregations to participate in wholesale energy, capacity, and ancillary services markets. Any future District framework addressing aggregator command authority and telemetry ownership (Section 5.7) should account for this existing federal layer: aggregators participating in PJM markets are already subject to Order 2222's registration and performance requirements, which provide a starting point for, rather than a substitute for, the District-specific cybersecurity governance questions raised in this paper.

5. CYBERSECURITY GOVERNANCE FRAMEWORK FOR FUTURE DER-ENABLED DISTRIBUTION SYSTEMS

5.1 SECURE COMMUNICATIONS ARCHITECTURE

Secure communications architectures are foundational to future DER interoperability environments. Relevant frameworks include IEEE 2030.5 [10], IEC 62351 [13], DNP3 Secure Authentication (IEEE 1815) [11], and Transport Layer Security (TLS).

- Secure communications architectures supporting interoperability functions
- Authenticated DER-to-utility communications
- Certificate lifecycle management
- Communications encryption and integrity protections

5.2 NETWORK SEGMENTATION AND TRUST BOUNDARIES

IEC 62443 [12] introduces security zones and conduits that establish trust boundaries between interconnected systems. Table 4 presents a representative trust-zone structure for a District DER architecture, from the customer-owned DER through aggregator and DERMS platforms to utility OT/SCADA.

Table 4. *Representative trust-zone architecture for DER-to-utility communications, based on IEC 62443 zone-and-conduit principles.*

Trust Zone	Representative Assets	Boundary Control
Customer / DER zone	Inverter, BESS controller, local DER communication interface (IEEE 1547-2018 Clause 10.1)	Device-level authentication, secure boot, local firewall
Aggregator / VPP zone	Aggregator platform, cloud dispatch service, third-party APIs	API security, certificate-based authentication, contractual cybersecurity terms
DERMS / ADMS zone (utility-operated)	DERMS application, telemetry historian, forecasting engine	IEC 62443 zones and conduits, Zero Trust access, SBOM-verified software
Utility OT / SCADA zone	SCADA, protection and control systems, grid-forming inverter coordination	Physical and logical segmentation from all zones above, DMZ brokered communications

5.3 AUTHENTICATION, IDENTITY MANAGEMENT, ACCESS CONTROL, AND ZERO TRUST

As operational interactions among DER assets, utilities, aggregators, and third-party service providers become more sophisticated, identity management and access governance become increasingly important. IEC 62443 [12], NIST SP 800-82 [14], and related frameworks emphasize role-based access control, least-privilege principles, multi-factor authentication, credential management, and operational authorization. A Zero Trust Architecture, in which no device, user, or platform is implicitly trusted regardless of network location and every operational command is authenticated and authorized individually, is a natural organizing principle for this environment given the multi-party structure described in Table 2: no single utility network perimeter can reasonably be trusted to separate authorized aggregator commands from unauthorized ones, since aggregators, DERMS platforms, and DER devices all sit, by design, outside the utility's traditional OT perimeter.

- Certificate-based authentication
- Role-based access controls, applied under Zero Trust principles rather than implicit network-location trust
- Multi-factor authentication
- Credential lifecycle management
- Operational command authorization, continuously verified rather than granted once at connection time

5.4 ADVANCED INVERTER SETTINGS GOVERNANCE, FIRMWARE, AND SECURE BOOT

Advanced inverter technologies increasingly support configurable functions directly influencing distribution system performance: Volt-VAR control, Volt-Watt functionality, ride-through settings, frequency response, reactive power support, and export management logic. Governance mechanisms for configuration management, settings validation, firmware updates, and operational accountability are needed, informed directly by the settings-manipulation vulnerabilities documented in Section 3.8. Secure boot, verifying that inverter and DERMS-gateway firmware has not been tampered with before it executes, is a device-level control that directly addresses the firmware-integrity dimension of that same risk and should be treated as a baseline expectation for new advanced inverter procurement, alongside signed firmware update packages and rollback protection.

- Configuration management procedures
- Firmware update governance, including signed updates and secure boot verification
- Settings validation processes
- Auditability and operational accountability frameworks

5.5 EVENT LOGGING, MONITORING, AND OPERATIONAL AUDITABILITY

Operationally interconnected DER environments depend on visibility into communications activities, telemetry exchanges, operational commands, and system events. Logging and monitoring capabilities support operational investigations, interoperability validation, incident response, disturbance analysis, and cybersecurity investigations.

- Operational event logging
- Communications activity monitoring
- Audit trail retention
- Firmware and configuration tracking

5.6 INCIDENT REPORTING AND OPERATIONAL RESPONSE

As DER interoperability expands, cybersecurity incidents may involve multiple stakeholders: utilities, DER owners, aggregators, equipment manufacturers, cloud service providers, and third-party operators. Clearly defined incident reporting procedures, communications protocols, escalation pathways, operational isolation strategies, and recovery planning support this multi-party reality, mapped to the coping/recovery role distinction in Table 2.

- Cyber incident notification procedures

- Escalation pathways and coordinated operational response
- Operational isolation strategies
- Recovery planning and restoration processes

5.7 DERMS, AGGREGATORS, THIRD-PARTY GOVERNANCE, AND API SECURITY

Future DERMS-enabled environments involve increasingly complex operational relationships among utilities, aggregators, VPP operators, cloud service providers, and customer-owned resources, mediated in practice through application programming interfaces (APIs) connecting aggregator platforms, DERMS applications, and utility systems. API security, authenticated and rate-limited endpoints, input validation to prevent injection of malformed commands, and API-level logging distinct from application-level logging, is therefore a direct technical requirement of the operational-authority and command-hierarchy questions this section raises, not a separate IT concern. The Forescout SUN: DOWN research (Section 3.8) documented exactly this failure mode: insecure direct object reference vulnerabilities in aggregator cloud APIs that allowed unauthorized access to connected inverter controls.

- Operational authority definitions and command hierarchy structures
- Telemetry ownership and data governance frameworks
- API authentication, rate-limiting, and input validation for all DERMS/aggregator/utility interfaces
- Cybersecurity accountability allocation, consistent with FERC Order 2222's existing aggregator framework (Section 4.6)

5.8 OPERATIONAL RESILIENCE AND CONTINUITY OF SERVICE

Cybersecurity governance ultimately supports reliability, resilience, and continuity of operations. Future high-DER operating environments increasingly depend on secure fallback modes, communications-loss procedures, autonomous operation capabilities, islanding coordination, restoration support, and continuity planning, especially important for resilience hubs, battery storage systems, microgrids, and grid-forming inverter deployments.

- Fail-safe operating modes and communications-loss response procedures
- Autonomous fallback operation and intentional islanding coordination
- Continuity of operations planning

5.9 SECURE-BY-DESIGN PRINCIPLES AND SUPPLY CHAIN / SBOM GOVERNANCE

Secure-by-Design, the principle, formalized in CISA's 2023 Secure by Design pledge program [8], that manufacturers should build security into products by default rather than treating it as a customer-configured add-on, applies directly to the DER manufacturer role in Table 2. For the District's interconnection process, this translates into a preference, over time, for advanced inverters and DERMS gateways procured from manufacturers that publish a Software Bill of Materials (SBOM), disclosing the third-party software components embedded in device firmware, participate in coordinated vulnerability disclosure programs, and ship with secure defaults (no default credentials, encrypted communications enabled out of the box) rather than requiring the installer to enable security features manually. Vendor risk management processes, evaluating a manufacturer's patch cadence, SBOM transparency, and disclosure history before procurement, complement this principle and are a direct, actionable response to the supply-chain risk documented in Section 3.6 and 3.8.

5.10 DEFENSE IN DEPTH AS AN INTEGRATING PRINCIPLE

No single control in Sections 5.1 through 5.9, secure communications, segmentation, Zero Trust access, secure boot, logging, incident response, API security, or Secure-by-Design procurement, is sufficient in isolation. Defense in Depth, layering independent controls so that the failure of any single layer does not result in a complete compromise, is the principle that ties Table 4's trust-zone architecture together: a compromised customer-owned inverter (Section 3.2, 3.8) should be contained by network segmentation (5.2) even if device-level secure boot (5.4) is bypassed; a compromised aggregator API (5.7) should be contained by DERMS-side Zero Trust access controls (5.3) even if the aggregator's own authentication is compromised. This is the structural argument for treating cybersecurity as foundational infrastructure, comparable to protection systems and voltage regulation equipment, rather than a checklist applied at any single point in the DER lifecycle.

6. TELEMETRY INTEGRITY AND OPERATIONAL DATA VALIDATION

The increasing deployment of DERs, advanced inverter technologies, BESS, and future DERMS-enabled operating environments is driving greater reliance on telemetry as a foundational component of modern utility operations.

6.1 TELEMETRY AS A CRITICAL OPERATIONAL ASSET

Telemetry serves as the operational bridge between distributed resources and utility decision-making. Future DERMS-enabled environments may utilize telemetry data to support monitoring, situational awareness, export management, forecasting, voltage management, DER coordination, and operational planning.

6.2 DATA INTEGRITY AND TRUSTWORTHINESS

Reliable utility operations depend on confidence in the accuracy and integrity of operational information. Telemetry that is inaccurate, manipulated, delayed, incomplete, or inconsistent may reduce operational visibility and affect decision-making.

6.3 FALSE DATA INJECTION AND OPERATIONAL DECISION RISK

Future DERMS-enabled environments may become dependent on operational information from thousands of interconnected devices. False data injection, erroneous telemetry, communications failures, synchronization errors, or compromised operational information could affect situational awareness and decision-making.

6.4 TIME SYNCHRONIZATION AND OPERATIONAL ACCURACY

Accurate timestamps support event reconstruction, operational investigations, disturbance analysis, interoperability verification, and incident response. Inconsistent timing information may complicate efforts to understand operational events or validate system performance.

6.5 TELEMETRY VALIDATION AND QUALITY ASSURANCE

Validation processes, verification of communications functionality, measurement accuracy, data completeness, operational availability, and performance consistency, are important components of future interoperability frameworks.

6.6 TELEMETRY AND DERMS-ENABLED GRID OPERATIONS

Future DERMS readiness depends not only on deployment of software platforms and communications infrastructure but also on the availability of reliable, secure, validated, and trustworthy operational information, especially as the District continues to advance distributed solar generation, battery storage deployment, and broader grid modernization objectives.

7. CONCLUSIONS AND NEXT STEPS

The future distribution system will increasingly depend on secure interactions among thousands of interconnected DERs, advanced inverters, DERMS platforms, aggregators, telemetry systems, and utility operational networks. This paper has argued three things beyond what its Executive Summary states: that IEEE 1547-2018 and IEEE 1547.3-2023 together define a complete but currently under-utilized structure for District cybersecurity governance (Section 2); that the risks this structure addresses are documented and current, not hypothetical, as the SUN:DOWN precedent demonstrates (Section 3.8); and that the District's own regulatory and procurement activity, Formal Case No. 1050's Order No. 22745 [4], the Local Solar Expansion Act's 15%-by-2041 target [5], and DOEE's July 2026 distributed battery storage RFI [6], already provides concrete, near-term opportunities to apply that structure rather than waiting for a future proceeding. This structure is consistent with the broader distributed-system planning practices catalogued by the Energy Systems Integration Group [26].

Three near-term next steps follow directly from this analysis:

1	**Reference the standards structure directly.** DOEE and the Commission could reference Table 1's category structure and Table 2's stakeholder matrix when scoping any future cybersecurity-focused technical conference under Formal Case No. 1050 or a successor docket, so that discussion is organized around IEEE 1547.3-2023's existing structure rather than built from a blank page.
2	**Fold Secure-by-Design into procurement.** Any forthcoming procurement guidance connected to DOEE's distributed battery storage RFI could reference the Secure-by-Design and SBOM expectations in Section 5.9 as evaluation criteria.
3	**Pilot the responsibility split informally.** The utility-owned versus customer-owned responsibility split proposed in Section 4.5 could be piloted informally, through the discussion questions in Appendix A, before any formal rulemaking is considered.

High-DER feeders, resilience hubs, grid-forming inverter deployments, VPP environments, DERMS-integrated systems, and future AI-enabled grid operations are where these considerations become most

concrete for the District specifically, and each is addressed as it applies to DOEE's Grid Modernization Initiative below.

High-DER Feeders

Within the District, high-DER feeders are distribution circuits experiencing increasing penetration of rooftop solar, community renewable energy facilities (CREFs) interconnected under Rulemaking 40 [27], BESS, EV charging infrastructure, and other DERs. As local solar deployment expands toward the District's 15% local generation target established by the Clean Energy DC Omnibus Amendment Act of 2018 [28] and the Local Solar Expansion Amendment Act of 2022 [5], these feeders are expected to experience greater bidirectional power flow, voltage regulation challenges, hosting capacity constraints, and operational complexity, consistent with the goals set out in Clean Energy DC 2.0 [29].

Resilience Hubs

Resilience hubs are strategically located community facilities capable of maintaining critical services during prolonged grid disruptions, potentially incorporating solar generation, battery storage, advanced controls, and microgrid capabilities. Within DOEE's energy assurance and resilience planning, resilience hubs represent an important strategy for protecting vulnerable populations and supporting continuity of government functions during extreme weather events, cyber incidents, or other large-scale disruptions.

Grid-Forming Inverter Deployments

Grid-forming inverters are capable of establishing voltage and frequency references, supporting black-start functionality, and maintaining stable operation in weak-grid or island conditions, and could support advanced microgrids, resilience hubs, intentional islanding strategies, and future distributed energy systems capable of providing grid-support services within the District.

Virtual Power Plant (VPP) Environments

Future VPP environments in the District would aggregate rooftop solar, battery storage, electric vehicles, demand response assets, and controllable loads into coordinated portfolios, functioning collectively to support peak demand reduction, capacity needs, resilience, voltage management, and system flexibility, subject to the FERC Order 2222 [25] framework discussed in Section 4.6.

DERMS-Integrated Systems

A DERMS would provide utilities and operators with enhanced visibility, coordination, and control of DERs across the distribution network, supporting advanced inverter functionality under IEEE 1547-2018, dynamic hosting capacity management, and coordination with battery storage and demand response resources.

Future AI-Enabled Grid Operations

Artificial intelligence and machine learning technologies have the potential to improve forecasting, outage prediction, anomaly detection, asset management, DER dispatch optimization, cybersecurity monitoring, and system restoration, while introducing their own cybersecurity considerations, including the integrity of training data and the risk of adversarial manipulation of AI-driven operational decisions, that should be addressed as this capability matures rather than assumed away.

The considerations presented throughout this paper should be viewed as part of a broader conversation regarding the future evolution of District distribution system operations. Continued stakeholder engagement through future proceedings, technical working groups, utility planning efforts, and resilience initiatives can help ensure the District remains well positioned to support reliable, resilient, secure, and equitable integration of distributed energy resources over the coming decades. Appendix A contains

discussion questions to assist stakeholders in evaluating these considerations; Appendix B contains discussion questions oriented toward the Commission specifically.

ACKNOWLEDGMENT

This research was supported in part by an appointment with The Clean Energy Innovators Fellowship program sponsored by the U.S. Department of Energy (DOE), administered by the Oak Ridge Institute for Science and Education (ORISE) for the DOE. ORISE is managed by Oak Ridge Associated Universities (ORAU) under DOE contract number DE-SC0014664. All opinions expressed in this paper are the author's and do not necessarily reflect the policies and views of DOE, ORAU, or ORISE.

REFERENCES

1. Institute of Electrical and Electronics Engineers. IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces; IEEE Std 1547-2018; IEEE: New York, NY, 2018.

2. Institute of Electrical and Electronics Engineers. IEEE Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems; IEEE Std 1547.3-2023; IEEE: New York, NY, approved June 5, 2023, published December 11, 2023.

3. National Institute of Standards and Technology. The NIST Cybersecurity Framework 2.0; NIST CSWP 29; U.S. Department of Commerce: Gaithersburg, MD, 2024.

4. Public Service Commission of the District of Columbia. Formal Case No. 1050, Investigation into the Implementation of Interconnection Standards in the District of Columbia, including Order No. 22745 (November 2025); DCPSC: Washington, DC.

5. District of Columbia Council. Local Solar Expansion Amendment Act of 2022 (15% local solar by 2041); Washington, DC, 2022.

6. District of Columbia Department of Energy and Environment. RFI: Commercial-Scale Distributed Battery Storage in the District; DOEE: Washington, DC, July 2026.

7. Forescout Technologies, Vedere Labs. SUN: DOWN: Destabilizing the Grid via Orchestrated Exploitation of Solar Power Systems; Forescout: San Jose, CA, March 2025.

8. Cybersecurity and Infrastructure Security Agency. Secure by Design Pledge; U.S. Department of Homeland Security: Washington, DC, 2023.

9. Public Service Commission of the District of Columbia. Formal Case No. 1163, [microgrid policy]; DCPSC: Washington, DC.

10. Institute of Electrical and Electronics Engineers. IEEE Standard for Smart Energy Profile Application Protocol; IEEE Std 2030.5-2018; IEEE: New York, NY, 2018.

11. Institute of Electrical and Electronics Engineers. IEEE Standard for Electric Power Systems Communications, Distributed Network Protocol (DNP3); IEEE Std 1815; IEEE: New York, NY.

12. International Society of Automation / International Electrotechnical Commission. Security for Industrial Automation and Control Systems; IEC 62443 Series; IEC: Geneva, Switzerland.

13. International Electrotechnical Commission. Power Systems Management and Associated Information Exchange, Data and Communications Security; IEC 62351 Series; IEC: Geneva, Switzerland.

14. National Institute of Standards and Technology. Guide to Operational Technology Security; NIST Special Publication 800-82, Revision 3; U.S. Department of Commerce: Gaithersburg, MD, 2023.

15. Institute of Electrical and Electronics Engineers. IEEE Application Guide for IEEE Std 1547; IEEE Std 1547.2; IEEE: New York, NY.

16. Institute of Electrical and Electronics Engineers. IEEE Standard Conformance Test Procedures for Equipment Interconnecting Distributed Energy Resources with Electric Power Systems and Associated Interfaces; IEEE Std 1547.1-2020; IEEE: New York, NY, 2020.

17. Underwriters Laboratories. UL 1741 Standard for Inverters, Converters, Controllers and Interconnection System Equipment for Use with Distributed Energy Resources; UL: Northbrook, IL.

18. Underwriters Laboratories. UL 2941, Distributed Energy Resources Cybersecurity (in development); UL: Northbrook, IL.

19. North American Electric Reliability Corporation. Critical Infrastructure Protection (CIP) Reliability Standards, including CIP-003 (Security Management Controls); NERC: Atlanta, GA.

20. International Electrotechnical Commission. Communication Networks and Systems for Power Utility Automation; IEC 61850 Series; IEC: Geneva, Switzerland.

21. U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response. Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid; U.S. DOE: Washington, DC.

22. U.S. Department of Energy and National Association of Regulatory Utility Commissioners. Cybersecurity Baseline for Electric Distribution Systems and Distributed Energy Resources; U.S. DOE/NARUC: Washington, DC.

23. Cybersecurity and Infrastructure Security Agency. Cross-Sector Cybersecurity Performance Goals; U.S. Department of Homeland Security: Washington, DC.

24. Potomac Electric Power Company. Small Generator Interconnection Procedures and Technical Filings Submitted in Formal Case No. 1050 and Rulemaking 40; DCPSC: Washington, DC.

25. Federal Energy Regulatory Commission. Order No. 2222, Participation of Distributed Energy Resource Aggregations in Markets Operated by Regional Transmission Organizations and Independent System Operators; FERC: Washington, DC, September 17, 2020.

26. Energy Systems Integration Group. Grid Planning and Operational Considerations for Distributed Energy Resources, Active Distribution Systems, and Large Loads; ESIG: Reston, VA.

27. Public Service Commission of the District of Columbia. Rulemaking 40: District of Columbia Small Generator Interconnection Rules; DCPSC: Washington, DC.

28. District of Columbia Council. Clean Energy DC Omnibus Amendment Act of 2018; D.C. Law 22-257; Washington, DC, 2019.

29. District of Columbia Department of Energy and Environment. Clean Energy DC 2.0: The District of Columbia Climate and Energy Action Plan; DOEE: Washington, DC, 2023.

APPENDIX A: Stakeholder Discussion Questions

Stakeholder Discussion Questions for DER Interoperability, Cybersecurity, and Grid Modernization Considerations

A.1 Secure Communications Architecture

1. Does Pepco currently require secure or encrypted communications protocols for DER operational interfaces participating in interoperability or telemetry functions?
2. Are IEEE 1547-2018 communications and interoperability capabilities integrated through secure DERMS or intermediary gateway architectures?
3. Does Pepco reference standards such as IEEE 2030.5, IEC 62351, or DNP3 Secure Authentication within operational DER communications environments?
4. How does Pepco evaluate cybersecurity risks associated with third-party DER communications platforms or aggregators?

A.2 Network Segmentation

5. How does Pepco architecturally separate DER communications environments from utility operational technology or SCADA systems?
6. Are intermediary DERMS or secure gateway architectures utilized to prevent direct DER exposure into operational utility environments?
7. Are segmentation requirements incorporated into operational interoperability governance procedures?
8. How are third-party DER aggregators or VPP operators isolated from core operational utility systems?

A.3 Authentication, Access Control, and Zero Trust

9. Are certificate-based authentication mechanisms required for DER operational communications?
10. How are operational permissions and command authorities governed for DER operational interfaces?
11. Are cybersecurity access control requirements defined for aggregators or third-party DER operators, and are they evaluated under Zero Trust assumptions rather than implicit network trust?
12. Does Pepco maintain credential lifecycle management or operational authorization governance procedures?

A.4 Inverter Settings Governance

13. How does Pepco govern post-interconnection modifications to advanced inverter operational settings?

14. Are firmware updates or remote parameter modifications subject to utility notification, secure boot verification, or other verification procedures?
15. Does Pepco maintain visibility into modifications affecting IEEE 1547-2018 grid-support functionality?
16. How are cybersecurity risks associated with remote inverter configuration managed operationally?

A.5 Event Logging and Operational Auditability

17. Does Pepco require operational logging capabilities for DER systems participating in utility-interactive programs?
18. Are communications events or operational command histories retained for investigations involving abnormal operational events?
19. How are interoperability failures or operational anomalies investigated from a cybersecurity perspective?
20. Are firmware or software version records maintained for operationally integrated DER systems?

A.6 Incident Reporting and Operational Response

21. Does Pepco maintain cybersecurity incident reporting requirements for DER operators or aggregators?
22. What operational procedures exist if a DER communications interface becomes compromised?
23. Are operational containment or coordinated utility isolation procedures defined for cybersecurity-related DER events?
24. How are cybersecurity incidents involving third-party operational platforms communicated to the utility?

A.7 DERMS, Aggregator, and API Governance

25. Does Pepco utilize or reference IEC 62443 principles, security zones and conduits, or other industrial control system cybersecurity frameworks when designing and governing DERMS, telemetry, and operational interoperability architectures?
26. Are API-level authentication, rate-limiting, and input validation requirements defined for aggregator and DERMS platform interfaces?
27. How does Pepco define operational command authority between the utility, aggregators, and DER operators, and how does this align with FERC Order 2222?
28. Are cybersecurity responsibilities contractually defined for third-party operational platforms?
29. Does Pepco maintain override authority during abnormal operational or cybersecurity events?
30. How are telemetry ownership and operational accountability governed?
31. Is Pepco positioned to implement the IEEE 1547.3-2023 guide, including its base and enhanced recommendation tiers?

A.8 Operational Resilience

32. How does Pepco evaluate operational resiliency during DER communications failures?
33. Are fallback operational modes required during communications disruptions?

34. How are cybersecurity protections integrated into intentional islanding or resilience hub operations?
35. Are black-start coordination procedures evaluated from both operational and cybersecurity perspectives?

A.9 Cybersecurity, Interoperability, Supply Chain, and DERMS Governance

36. Does Pepco currently reference IEC 62443, NIST SP 800-82, DOE CESER guidance, or other industrial control system cybersecurity frameworks when evaluating DER interoperability, telemetry, DERMS integration, or operational technology architectures?
37. How does Pepco evaluate cybersecurity risks associated with DER aggregators, third-party communications platforms, cloud-based operational services, and DERMS-integrated environments?
38. Are there existing utility standards, procurement requirements, or operational governance processes that address secure lifecycle management, software updates, firmware validation, SBOM transparency, vendor risk management, or supply-chain cybersecurity for DER interoperability technologies?
39. As IEEE 1547-2018 interoperability capabilities become more widely deployed, does Pepco anticipate additional cybersecurity, communications, or operational governance requirements beyond those currently addressed through interconnection procedures?

APPENDIX B: Commission Discussion Questions

As the District advances IEEE 1547-2018 implementation, increasing DER penetration, advanced inverter deployment, energy storage integration, and future DERMS-enabled operations, the following questions may warrant future Commission consideration.

B.1 Cybersecurity Governance and Operational Technology Security

1. How does the Commission envision addressing cybersecurity governance associated with IEEE 1547.3-2023, communications interoperability, operational technology security, and DERMS integration considerations associated with IEEE 1547-2018-enabled resources as DER adoption continues to expand?
2. To what extent should cybersecurity, interoperability, and operational technology considerations be incorporated into future grid modernization planning supporting advanced inverter deployment, DERMS readiness, resilience initiatives, and high-DER distribution system operations?
3. How can the Commission ensure that future efforts to streamline interconnection timelines, reduce project costs, and accelerate DER deployment do not unintentionally weaken cybersecurity protections, interoperability validation processes, or critical infrastructure security objectives?

B.2 Interoperability and Communications Architecture

4. Does the Commission anticipate establishing future expectations related to interoperability, communications architectures, telemetry performance, or operational visibility as advanced inverter capabilities become more widely deployed?
5. How should future interconnection regulations, utility implementation plans, or grid modernization initiatives address secure communications architectures, authenticated DER-to-utility interfaces, certificate management, and interoperability verification?

6. What role should standards such as IEEE 2030.5, IEC 61850, and IEC 62351 play in supporting secure and scalable DER integration?

B.3 Advanced Inverter Governance and DERMS Readiness

7. As DER systems increasingly support telemetry, export management, remote configuration, advanced grid-support functionality, and future DERMS integration, how should governance responsibilities be allocated among utilities, DER owners, aggregators, equipment manufacturers, and third-party service providers, consistent with the role-mapping proposed in Section 4.5?
8. Does the Commission anticipate future consideration of governance frameworks addressing inverter settings management, firmware lifecycle oversight, telemetry validation, operational authority, and cybersecurity accountability for interconnected DER assets?
9. How should future DERMS-enabled operating environments balance operational flexibility, cybersecurity protections, customer participation, and utility reliability requirements?

B.4 Future High-DER Distribution System Operations

10. As the District advances community solar deployment, battery storage integration, resilience hubs, microgrids, vehicle-to-grid technologies, and virtual power plant participation, what operational governance considerations may become increasingly important to maintaining reliability, resilience, and cybersecurity?
11. How can lessons learned from industrial control system cybersecurity frameworks, operational technology security practices, and electric sector reliability standards inform future high-DER distribution system planning?
12. What additional stakeholder engagement, technical studies, pilot programs, or implementation planning activities, including a possible pilot of the DOEE distributed battery storage RFI's cybersecurity procurement criteria, may be beneficial to support secure, interoperable, and resilient DER integration over the long term?

This white paper was developed to support ongoing efforts to strengthen the cybersecurity, interoperability, operational resilience, and cyber-physical security of distributed energy resources interconnected with the District of Columbia's electric distribution system. It provides a strategic framework for utilities, regulators, policymakers, technology providers, equipment manufacturers, DER owners, aggregators, and other stakeholders involved in implementing IEEE 1547-2018 and IEEE 1547.3-2023, while advancing grid modernization, secure DER integration, DERMS readiness, and the resilience of the District's critical energy infrastructure.