Commonwealth of Virginia
STATE CORPORATION COMMISSION

DAVID ESSAH, Ph.D.
DIRECTOR

DIVISION OF
PUBLIC UTILITY REGULATION
P.O. Box 1197
Richmond, Virginia
23218-1197
(P) 804-371-9611
(F) 804-371-9350

November 25, 2025

BY ELECTRONIC MAIL

The Honorable Jeion A. Ward
Member, Virginia House of Delegates
Chair, Committee on Labor and Commerce
P.O. Box 7310
Hampton, Virginia 23666
DelJWard@house.virginia.gov

The Honorable R. Creigh Deeds
Member, Senate of Virginia
Chair, Committee on Commerce and Labor
P.O. Box 5462
Charlottesville, Virginia 22905
senatordeeds@senate.virginia.gov

Dear Delegate Ward and Senator Deeds:

This correspondence provides the Report of a working group on the Evaluation of Cybersecurity in Relation to the Provision of Electric Service by Investor-owned Incumbent Electric Utilities and Electric Cooperatives convened pursuant to Chapter 444 of the 2025 Virginia Acts of Assembly (SB1239),and led by the Staff of the State Corporation Commission's Division of Public Utility Regulation.

A comprehensive summary of the working group, including an overview of each presentation and the subsequent Q&A session, is provided in the Report, followed by the findings and recommendations.

Please let us know if you need additional information or assistance.

Respectfully submitted,

David N. Essah

David N. Essah, Ph.D.

cc: The Honorable Ryan T. McDougle

Attachments

COMMONWEALTH OF VIRGINIA

STATE CORPORATION COMMISSION

Reports to the Chairmen of the House Committee on Labor and Commerce
and the Senate Committee on Commerce and Labor

Report on the Evaluation of Cybersecurity in Relation to the Provision of Electric Service by Investor-owned Incumbent Electric Utilities and Electric Cooperatives Pursuant to Chapter 444 of the 2025 Virginia Acts of Assembly (SB1239)

November 25, 2025

Table of Contents

I. BACKGROUND

Chapter 444 (Senate Bill 1239) of the 2025 Virginia Acts of Assembly directs the State Corporation Commission ("Commission") to convene a work group to evaluate cybersecurity in relation to the provision of electric service by investor-owned incumbent electric utilities and electric cooperatives. Under Chapter 444, the work group is required to consider:

i. Actions that an investor-owned electric utility or electric cooperative may take if a customer experiences an emergency condition that, as determined by the utility or cooperative, could compromise the reliability or security of electric service to other customers; and
ii. Any other topics the Commission deems relevant.

In addition, the Commission is tasked with facilitating and documenting the work group's proceedings. Chapter 444 requires the Commission to submit a written report, including any findings and recommendations, to the Chairmen of the House Committee on Labor and Commerce and the Senate Committee on Commerce and Labor by November 30, 2025. The Commission must also make the report publicly available on its website at the same time.

Pursuant to these statutory directives, on July 7, 2025, the Staff of the Commission ("Staff") convened a virtual work group to address cybersecurity and any other relevant topics as they pertain to electric service by Virginia's investor-owned electric utilities and electric cooperatives. The work group featured presentations from the following entities:

- U.S. Department of Homeland Security ("DHS")
- Federal Bureau of Investigation ("FBI" or "Bureau"), Richmond Division
- SERC Reliability Corporation ("SERC")
- Virginia Electric Power and Company d/b/a Dominion Energy Virginia ("Dominion")

A list of all entities participating in the working group can be found in Attachment 1 to this report.

A comprehensive summary of the working group, including an overview of each presentation and the subsequent Q&A session, is provided below. This is followed by the corresponding findings and recommendations.

II. WORKING GROUP DISCUSSIONS

DHS – Datacenter Primer

DHS's presentation focused on its perspective regarding data center threats from nation-state actors. DHS asserts that hostile foreign actors are leveraging advanced, whole-of-government capabilities to target U.S. data centers for both economic and security advantages, including

intellectual property theft and disruption of government or corporate assets. DHS notes that adversaries are interested in both sensitive government information and intellectual property,

recognizing that data centers are critical elements of U.S. technological and economic infrastructure.

According to DHS, a significant portion of global internet traffic flows through the Northern Virginia data corridor, which it views as a unique vulnerability. The agency highlights that adversarial nations may target data centers to gain access to data or to secure critical technologies such as advanced semiconductors. DHS asserts that the load demands created by data centers, including those driven by Artificial Intelligence ("AI") training and cryptocurrency mining, present further operational and security challenges for the electric grid.

DHS states that data centers, with their physical presence and role in managing vast amounts of information, are highly attractive targets for both state and criminal actors. These actors may pursue data for espionage, financial gain, or to exploit U.S. infrastructure. DHS raises concerns over direct foreign investment and technology transfers, especially where data centers are located near sensitive U.S. assets. DHS references prior cases, such as an executive order blocking the construction of a crypto mining facility owned by nationals of the People's Republic of China near the Francis E. Warren Air Force Base in Cheyenne, WY, to illustrate the national security risks posed by foreign-controlled facilities.

DHS emphasizes the diversity of data center types—enterprise, colocation, hyperscale, modular—and highlights that these centers store information supporting activities ranging from government operations to e-commerce. DHS warns that compromised supply chains and counterfeit parts may also allow adversaries to infiltrate otherwise secure data centers. DHS also draws attention to threats posed by advanced AI model training and by actors manipulating data center load to disrupt grid reliability.

DHS concludes that protecting data centers from foreign adversaries, supply chain threats, illicit investment, and cyber intrusions is crucial to U.S. national and economic security. The agency encourages vigilance and information sharing, noting that the private sector owns most U.S. critical infrastructure. DHS represents that continued engagement with federal partners is essential, particularly as hostile entities seek to exploit emerging vulnerabilities.

FBI – Large Load Threats to the Bulk Power System

FBI states that the rapid growth of large loads, driven in part by data centers, AI, and new technologies, places unprecedented strain on the electric grid and presents unique national security risks. The FBI asserts that while reliability is typically assumed by most Americans, it is threatened by evolving cyber and physical threats.

FBI representatives emphasize that a lack of consistent federal standards for large load interconnection, insufficient load modeling, and routine equipment failures all contribute to potential vulnerabilities in the operation of data centers. The FBI specifically highlights risks identified in recent Northern Virginia data center incidents, where unplanned load drops have demonstrated how sudden fluctuations can impact the grid. These unplanned load drops are discussed in detail later in the Report

FBI asserts that its mission includes close engagement with energy sector partners. The Bureau urges utilities to consider not only the likelihood of cyber threats, but also the potential impact adversaries could achieve if determined to target the sector. FBI mentions that adversaries such as Russia, Iran, and especially China, target the bulk power system to achieve geopolitical leverage, disrupt military mobilization, or retaliate against U.S. influence abroad. The Bureau describes past Russian efforts to establish footholds in U.S. critical infrastructure and China's intent to maintain persistent presence as a deterrent to U.S. intervention in regional conflicts.

FBI notes that adversaries are likely to target energy assets near defense, government, and critical facilities. The Bureau references the possible use of compromised large loads, like hyper-scale data centers or crypto mining, to inflict outages or destabilize the grid. It notes particular concerns with Chinese-manufactured equipment. FBI asserts that adversarial access can be challenging to detect because of opaque investment structures and the integration of technology across the grid supply chain.

FBI encourages continued information sharing between utilities and the Bureau. The Bureau states it is committed to providing declassified intelligence, sponsoring security clearances for key infrastructure partners, and supporting efforts to understand and mitigate grid vulnerabilities. The Bureau concludes by reaffirming its partnership with utilities and its goal of raising awareness about adversary motivations, means, and methods in targeting the U.S. bulk power system.

Q&A Discussion with DHS and FBI

The Q&A session with DHS and FBI featured questions about the relative likelihood and risk assessment of accidental versus deliberate threats to data centers and the electric grid. Participants noted that non-malicious misuse or mis-operation, in addition to deliberate attacks, could lead to significant impact. DHS and FBI agreed that while many threats result from mistakes or accidents, the potential for deliberate hostile action by nation-state actors cannot be ignored.

DHS and FBI clarified that neither agency could prescribe exact best practices for utilities or private-sector partners but emphasized the importance of ongoing engagement, information sharing, and regular contact between utilities and both agencies, encouraging utilities to reach out with requests for additional guidance, and briefings when warranted.

One question addressed Executive Order 13873 and whether it provides an effective regulatory tool for securing the Information and Communications Technology (ICT) and hardware supply chain. DHS responded that this is a good question for the Cybersecurity and Infrastructure Security Agency (CISA) but reinforced the value of understanding one's supply chain, proactively auditing components, and not indiscriminately trusting third-party vendors. FBI and DHS recommended keeping informed about supply chain risks, emphasizing the importance of partnerships and the need for a collective approach to cybersecurity.

Participants also discussed societal and political challenges to highlighting supply chain risks, particularly those involving foreign-made components. DHS and FBI acknowledged these

complexities and encouraged attendees to leverage their perspectives and expertise to elevate the national security significance of such issues when advocating for risk mitigation.

Questions also touched on how Virginia could lead in securing its growing data center infrastructure without stifling economic growth. FBI described its role in vetting foreign investment through coordination with the Committee on Foreign Investment in the United States (CFIUS) and the process for providing recommendations on transactions that pose national security concerns.

The Q&A wrapped with a discussion of the importance of planning for both maximum and minimum load situations, and referenced ongoing task force and standards development work that aims to address these operational challenges and support system reliability.

SERC[1] – Updates on Inverter-Based Resources Large Load Task Force Activities

SERC stated that its role as one of the six North American Electric Reliability Corporation ("NERC") regional entities is to ensure the reliability and security of the bulk power system across 16 states, including Virginia. SERC described the formation of the Large Load Task Force ("LLTF") in August 2024 was to better understand and address the impacts of rapidly expanding large loads, such as data centers, on grid reliability.

SERC asserted that the LLTF is delivering two white papers and a reliability guideline to NERC registered entities, external entities, and broader groups. The first white paper, published in July 2025, identifies and prioritizes risks associated with large loads.[2] The second white paper, expected in Q3 2025, will assess whether existing engineering practices and standards can adequately capture these risks, particularly focusing on load modeling gaps.[3] SERC asserted that these analyses will support improvements in planning, operations, data collection, and event analysis, and will inform a new reliability guideline targeted for release in early 2026.

SERC noted certain specific high-priority risks as follows: (1) resource adequacy (ensuring sufficient generation to meet load); (2) balancing and reserves (maintaining production-consumption equilibrium despite quick load ramps); and (3) event ride-through (ensuring large loads stay online during faults or system events). SERC emphasizes the importance of improved information sharing between entities and customers to support forecasting, operational planning, and mitigation of reliability risks. Real-time monitoring and timely communication of operational data are also highlighted as important reliability tools.

---

[1] SERC is one of six companies that support the NERC Electric Reliability Organization (ERO) Enterprise. SERC is responsible for reliability and security across the southeastern and central regions of the United States. *See* https://www.nerc.com/who-we-are/key-players

[2] The first white paper, titled "Characteristics and Risks of Emerging Large Loads" (July 2025), is available at: https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Whitepaper%20Characteristics%20and%20Risks%20of%20Emerging%20Large%20Loads.pdf

[3] According to the information from the NERC Large Loads Task Force Meeting held on October 23, 2025, the second white paper is expected to be published in Q1 2026. *See* https://www.nerc.com/comm/RSTC/LLTF/LLTF_Presentations_October_23_2025.pdf

The market for inverter-based resources ("IBRs") has grown rapidly and significantly impacts system reliability.[4] SERC noted that from 2017 to 2021, the United States added the equivalent of 73 gigawatts of IBR generation. Despite this expansion, SERC observed that a gap in standards applicability exists because many IBRs are smaller facilities that previously fell outside the scope of NERC reliability standards.

According to SERC, approximately 84% of IBR generation is currently interconnected to the bulk electric system ("BES") and therefore subject to NERC standards. SERC stated that the definition of BES generation is any facility that is sized greater than 75 megavolt-amperes ("MVA") and interconnected at greater than 100 kilovolts ("kV"). SERC's analysis showed that lowering the applicability threshold to below the level that defines BES generation would capture more IBR sites and raise NERC standards coverage to nearly 98% of IBRs.[5] SERC asserts that this change has become necessary because even smaller aggregations of IBRs have contributed to bulk power system disturbances.

In order to close the gap, SERC explains that, in response to Federal Energy Regulatory Commission ("FERC") direction, NERC and its regions adopted a three-year, three-phase plan (May 2023 to May 2026) to bring more IBRs under the scope of NERC reliability standards by requiring their owners and operators to become registered entities.

SERC noted that the first phase of the plan, which began in May 2023, involved modifications to NERC's Rules of Procedure. Specifically, NERC amended the definitions of Generator Owner and Generator Operator. As stated above, previously, only facilities above 75 MVA and interconnected at greater than 100 kV (BES resources) were captured by these definitions. The updated definitions now cover IBR facilities with ratings greater than 20 MVA and interconnections at voltages above 60 kV, even if they are not classified as part of the bulk electric system.

The second phase focused on identifying and cataloging all IBR facilities that now meet the new registration criteria. SERC states that this effort included analyzing Department of Energy data and sending information requests to transmission owners and balancing authorities. This process ensures that regional entities have a comprehensive inventory of affected facilities before registration deadlines.

The third phase, running through May 2026, requires that all newly identified IBR owners and operators complete formal registration with their regional entity (such as SERC), making them subject to the full suite of NERC reliability standards. SERC states that by following this phased approach, NERC and its regions are closing reliability gaps for IBRs, as these resources become an increasingly significant share of generation on the interconnected grid.

[4] An IBR refers specifically to a generating unit that uses power electronic inverters, such as photovoltaic systems, to convert direct current (DC) into alternating current (AC). A distributed energy resource ("DER"), in contrast, is a broader classification that includes both inverter-based and non-inverter-based technologies. Accordingly, while all inverter-based DERs are IBRs, not all DERs are IBRs.

[5] The 98% coverage represents all IBRs of 20 MW or larger connected at any voltage level.

SERC concludes by encouraging ongoing collaboration, noting upcoming publications and webinars, and emphasizing that partnership and early communication across utilities, developers, and operators are essential to meeting the challenges posed by large, fast-growing loads on the grid.

Q&A Discussion with SERC

The Q&A following SERC's presentation focused on practical implementation and compliance questions regarding the new registration requirements for owners and operators of non-BES IBRs. Participants asked about the compliance implications for facilities that newly meet the lower threshold. SERC confirmed that new registrants will face compliance costs, including developing internal programs, procedures, documentation practices, and staff training. SERC states it has worked to proactively engage affected entities, especially those new to NERC compliance, by providing informational webinars and guidance to support a smooth transition and manage expectations about the regulatory process.

Questions were raised about which party is responsible for registration. SERC clarified that it is the owner or operator of the facility that becomes the NERC registered entity and not the distribution utility serving the facility.

Participants sought specifics regarding how standards would apply, such as the Critical Infrastructure Protection ("CIP") standards and supply chain requirements. SERC asserted that revisions to some of NERC standards are underway, particularly affecting applicability tables and control requirements for these newly registered non-BES (Category 2) IBRs. SERC indicated that applicability and required controls will be scaled according to facility risk, and that the current update process is tied to a multi-year FERC timeline for new and expanded standard submissions covering performance, modeling, operations, planning, and cybersecurity considerations.

Several questions focused on timing, impacts of the new compliance threshold for smaller IBRs, and coordination with other standards (such as IEEE[6]) for IBRs falling below NERC's scope. SERC stated that efforts are underway to monitor these issues and minimize conflicts across standards as much as possible. SERC further emphasized ongoing outreach and the role of its regional risk reports, as well as highlighting supply chain cyber risks and mitigation activities, both within and outside traditional compliance and monitoring.

Questions were asked about ride-through requirements for data centers and large loads. SERC and utility representatives described positive progress in partnership and collaboration to encourage customer adoption of practices that support grid reliability, with ongoing discussion around contract and operational expectations. Finally, when asked if new reliability requirements would fall only on utilities or also on large load customers, SERC explained that its current focus is on planning and utility practices, though input about potential load-side risk is being considered for future regional risk reports and guidelines.

[6] Institute of Electrical and Electronics Engineers.

Dominion – Large Load Drop Events, Lessons Learned, and Mitigation Strategies

Dominion's presentation addressed recent unplanned data center load drop events, lessons learned, and approaches to mitigate future occurrences. Dominion stated that data center load additions in its territory continue at a rapid pace, and five of the top ten system peaks occurred within two weeks during the June 2025 heatwave.

Dominion summarized two significant load drop events. First, in July 2024, a 230 kV transmission line outage caused by a failed lightning arrestor resulted in 1,551 megawatts ("MW") of data center load being dropped from the grid by data center operators and transferred to backup generation, as a protective measure (*i.e.*, self-isolation). Dominion also identified a separate incident in February 2025, when a 230 kV transmission line outage due to a tree strike led to 1,800 MW of data center load being similarly dropped from the grid and transferred to backup generation. Dominion stated that these events produced voltage spikes at multiple substations and required coordinated actions to maintain grid stability. Specifically, Dominion system operators disconnected capacitor banks in the impacted area to bring the voltages back within their normal ranges which, according to Dominion, is a normal process responsive to such events, and not considered a specific emergency procedure.

Dominion observed a range of responses from its data center customers during the aforementioned events, with some data centers riding through faults using an uninterruptible power supply ("UPS") or controller feedback, and others fully tripping offline after several reclosing cycles. Dominion stated that detailed point-of-interconnection data is critical to determine facility performance during such events.

Dominion identified several lessons from these events, including: the importance of dynamic data collection and analysis, clear ride-through requirements, delay logic requirements in agreements, and batch study approaches for modeling aggregate impacts. Dominion states that it is updating its interconnection requirements to include dynamic modeling, more robust load data, and a queue process for large new requests above 100 MW. Remedial actions include revising undervoltage relay settings and event timers to avoid unnecessary load transfers, and Dominion further recommends replacing electromechanical relays with digital relays at sites serving data centers.

Dominion stated that it has shared these experiences with industry partners and continues to work with utilities and organizations such as PJM,[7] NERC, and EPRI[8] to assess reliability risk, collect facility data, and improve coordination with large load customers.

Q&A Discussion with Dominion

The Q&A discussion with Dominion focused on collaboration, data center engagement, cybersecurity, and system stability. The Coalition commended Dominion for proactive communication and partnership throughout and after the 2024 – 2025 load drop events. Dominion

[7] PJM Interconnection, LLC.

[8] Electric Power Research Institute.

stated that it has worked closely with both affected and broader data center community to share lessons learned, understand voltage and operational sensitivities, and tailor facility interconnection requirements to reflect facility-specific operational data and settings.

Dominion noted that equipment failures are unavoidable, but reported early reliability improvements from collaborative efforts, which has led to a reported reduction of load drops in subsequent events due to customer-driven actions.[9] At the work group meeting, Dominion stressed the importance of balancing reliability and cost, updating standards to reflect evolving technology, and pursuing steady, deliberate progress. Future advancements, Dominion emphasized, will depend on continued data sharing and tailored analysis, given the unique design and operation of each facility. Dominion and the Coalition state that while the industry is not monolithic, the current collaborative approach fosters best practice sharing and reliable grid operation.

Relative to cybersecurity, Dominion and the Coalition stated that data centers take cyber protections seriously, with security forming a central aspect of contractual agreements. Dominion clarified that the BES is regulated by the NERC Reliability Standards for planning and operation and the CIP standards for cybersecurity. Dominion acknowledged that it is less regulated with respect to the distribution grid and would like deeper visibility on customer protections at the point of connection. Dominion's transmission and cyber teams continue to monitor and secure the Company's own assets, using advanced monitoring to detect changes in their environment and collaborating internally between cybersecurity, operational technology, and physical security teams.

Dominion confirmed that ongoing dynamic studies are being conducted to develop metrics to determine at what level of load drop system stability could become vulnerable. While recent events have not posed an emergency risk, Dominion stated that it is actively modeling "worst-case" load drops to define system thresholds.

Based on subsequent discussions with Dominion, the Company has identified the following actions which can be taken if a customer experiences an emergency condition that, as determined by Dominion, could compromise the reliability or security of electric service to other customers:

- Capacitor banks can be manually disconnected by utility operators to bring down voltages after the loss of a large load on a circuit.
- The use of Flexible AC Transmission System ("FACTS") devices, such as Static Synchronous Compensators ("STATCOM") and Static Var Compensators ("SVC") could be leveraged to automatically bring down voltages after the loss of a large load on a circuit. Such an approach could supplement or replace the need for switched capacitor banks.

[9] Notably, on June 19, 2025, after the work group meeting, another fault occurred on the same transmission line as the February 2025 load loss event. While approximately 1,300 MW of data center load across 20 Dominion facilities instantly transferred to backup power due to the resulting voltage sag, voltages quickly returned to normal, allowing data centers to all transfer back to utility power within 20 to 90 seconds. This significantly improved response, Dominion asserts, was made possible through utility coordination with these data centers which had led to them using adjusted trip settings.

- Adjustments to utility reclosing standards could be made to better align with large load customers' facilities, thereby providing large load customers a better ability to ride through abnormal grid conditions.

Some of these actions were taken by the Company during the previously mentioned large load events.

NNEC and NOVEC – Cooperative Perspective

While the cooperatives did not give a formal presentation, representatives from NNEC and NOVEC were able to provide the work group with additional perspective, as discussed next.

Q&A Discussion with NNEC and NOVEC

Representatives from NNEC and NOVEC spoke to distinct challenges and priorities for electric cooperatives. NNEC highlighted that while operational and cybersecurity concerns are important, the cooperatives' immediate priority is financial risk; specifically, concerns about fair and equitable transmission cost allocation so that residential members are not disproportionately affected by large load growth. With data center interconnection requests vastly exceeding historical peak loads, the cooperative is focused on ensuring that new projects do not shift cost burdens unfairly. NNEC adds that maintaining tools and utility flexibility is crucial for rural areas, especially near sensitive sites such as military facilities. Partnerships are highlighted as being essential, including with Dominion, Old Dominion Electric Cooperative (ODEC), and other electric cooperatives.

NOVEC emphasized its strong working relationship with Dominion, including supporting data sharing, risk review, and mitigation strategies developed in response to recent events. NOVEC affirmed its support for Dominion's recommendations and continues to maintain close operational ties to manage large load integration risk.

Both electric cooperatives reiterate that managing unique community and location risks requires variety in planning, contracts, and grid solutions. They each describe ongoing internal discussions and communications with Dominion as being positive and supportive. The cooperatives also point out that while large-scale events may have a less immediate effect on their system than on Dominion's, their proportionate impact can be greater and demands close partnership and adaptable processes.

III. FINDINGS AND RECOMMENDATIONS

<u>Cybersecurity</u>

Based on comments and feedback received from the work group, a consensus exists between the work group and Staff, that cybersecurity is a risk to both NERC regulated, and non-NERC regulated entities, including interconnected local distribution networks and their customers' large loads.

With respect to NERC regulated entities, several comments were made by Dominion and SERC highlighting that there is currently ongoing work being conducted by the NERC LLTF to develop Reliability Guidelines identifying risk mitigation improvements to existing planning, and operation processes and interconnection requirements for large loads.[8] Staff understands that the guidelines are to address modeling practices, analyses, coordination and data collection efforts, real time monitoring, and event analysis for large loads. Staff believes it is important to consider the work being conducted by the LLTF when requiring utilities to develop independent related standards or guidelines, in order to avoid duplicative or conflicting requirements that could potentially impact reliability. Because NERC is not directly involved in regulating the local distribution or delivery of electricity,[10] there is a gap in regulatory coverage of cybersecurity risk, with respect to local distribution providers and their interconnection customers, which includes large loads and distributed energy resources. Staff has previously made cybersecurity related recommendations regarding DERs; specifically, in Case No. PUR-2023-00069, Staff recommended that:[11]

> "Each Utility shall establish its own utility-specific minimum cybersecurity standards based on and not in conflict with, nationally recognized guidelines, including but not limited to IEEE Standard 1547.3, Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems, 2023 and the National Association of Regulatory Utility Commissioners' Cybersecurity Baselines for Electric Distribution Systems and DERs. These standards shall also include requirements for testing, validation, and auditing of the implemented cybersecurity measures. Each Utility shall ensure these standards are publicly accessible by publishing them on their respective websites."

Similarly, relative to cybersecurity risks posed by interconnected large loads, Staff recommends based on the work group discussion that regulated utilities develop and implement *formal* plans addressing the actions the utilities may take if a customer experiences an emergency condition that, as determined by the utility or cooperative, could compromise the reliability or security of electric service to other customers, including those actions described in this report. Such plans should be updated where necessary, following an adverse event. Staff notes that Staff holds cybersecurity review meetings with regulated utilities on at least an annual basis, as such Staff recommends that utilities report the effectiveness of such plans to Staff on at least an annual basis, during these meetings.

---

[10] Section 215 of the Federal Power Act, codified at 16 U.S.C. § 824o. NERC, as designated by FERC, is explicitly responsible for developing and enforcing mandatory reliability and cybersecurity standards for the Bulk Electric System.

[11] *See Commonwealth of Virginia ex rel. State Corporation Commission, Ex Parte: In the matter of revising the Commission Regulations Governing Interconnection of Small Electrical Generators and Storage*, Case No. PUR-2023-00069, Doc. Con. Cen. No. 250720123, Staff Response of the Division of Public Utility Regulation (July 16, 2025), Attachment 1 at 3.

Large Load Growth Grid Impacts

The rapid proliferation of large loads, particularly data centers and cryptocurrency mining operations, poses significant challenges to electric grid reliability, planning, and operations, should such customers experience emergency conditions that compromise the reliability or security of electric service to the Commonwealth's regulated utilities. Presentations from DHS, FBI, SERC, and Dominion collectively underscore that these loads are not only increasing in scale and complexity but are also introducing new risk factors to the electric grid, including:

- *Sudden Load Drops*: As evidenced by Dominion's July 2024 and February 2025 events, unplanned disconnection of large loads can cause voltage instability, and they require an immediate grid response.
- *Inadequate Modeling and Forecasting*: Current planning and interconnection processes often lack sufficient dynamic modeling and real-time data to accurately predict large load behavior under fault or contingency conditions.
- *Cyber and Physical Security Risk Convergence*: Large loads, especially those with foreign investment or opaque ownership structures, may present both cybersecurity and physical reliability risks, as highlighted by DHS and FBI.

Given these various risk factors, utilities will need to be equipped to quickly respond to unplanned grid events when they occur, to maintain grid reliability. To date, Dominion has experienced a few such events and taken the necessary operational actions needed to bring grid conditions back to normal, as previously noted. Additional, *proactive* actions may be taken by utilities to eliminate or mitigate the potential grid impacts if a customer experiences an emergency condition. Some of these actions have indeed been successfully deployed by Dominion, as previously discussed. Such proactive actions could in part be informed by the results of the ongoing NERC LLTF study.

Accordingly, Staff makes the following recommendations:

- Relative to cybersecurity risks posed by interconnected large loads, it is recommended that regulated utilities develop and implement *formal* plans addressing the actions the utilities may take if a customer experiences an emergency condition that, as determined by the utility or cooperative, could compromise the reliability or security of electric service to other customers. Such plans should be updated where necessary, following an adverse event. Utilities should report the effectiveness of these plans to Staff on at least an annual basis.

- Utilities should revise their interconnection standards for large loads to include more robust technical requirements. These requirements should include dynamic modeling data, clearly defined ride-through capabilities, delay logic for event response, and real-time data monitoring. These enhancements will help ensure that large loads can remain stable and online during system disturbances and that utilities have the data needed to manage grid impacts effectively. Toward the same end, utilities should evaluate the use of high-fidelity metering and updated reclosing standards for high load customers where needed.

- Utilities should work with existing large load customers to adjust their equipment trip settings to allow for some level of ride-through capabilities. Dominion's recent coordination with large load customers has already shown promise in limiting grid disturbances during abnormal conditions.
- Improved coordination and data sharing between utilities and large load customers is essential. Utilities should establish formal agreements with large load customers that ensure timely access to customers' operational data, event logs, and telemetry. This will support more accurate load forecasting, faster responses to disturbances, and better alignment between customer operations and grid needs.
- Based on the recent large load events, utilities should evaluate the use of FACTS devices, such as STATCOM and SVCs to supplement or replace the process of switching capacitor banks for voltage control, to more rapidly correct for voltage swings in areas of high load, during emergencies.
- Staff supports the ongoing work of the NERC LLTF, particularly its forthcoming Reliability Guideline. Once published, utilities should align their planning and operational practices with LLTF recommendations, especially in areas such as load modeling, event ride-through expectations, and coordination with IBRs.
- Finally, utilities should provide annual reports to Staff detailing the number and size of large load interconnection requests, any operational incidents involving large loads, and their progress in implementing LLTF-aligned practices. This reporting will help track industry adoption and inform future policy decisions.

ATTACHMENT 1

List of Participating Entities

Appalachian Power Company

Craig-Botetourt Electric Cooperative

Data Center Coalition

Department of Homeland Security

Dominion Energy

Federal Bureau of Investigations

North American Electric Reliability Corporation

Northern Neck Electric Cooperative

Northern Virginia Electric Cooperative

Rappahannock Electric Cooperative

Shenandoah Valley Electric Cooperative

Solar Energy Industries Association

Southeastern Electric Reliability Corporation

State Corporation Commission

Virginia Energy

Virginia, Maryland & Delaware Association of Electric Cooperatives

Virginia Manufacturers Association