ELECTRICITY
ADVISORY
COMMITTEE

Resilient Communication for Grid Security: Enabling Private Broadband Networks for Critical Infrastructure

Electricity Advisory Committee
Recommendations for the
U.S. Department of Energy
June 05, 2025

Table of Contents

Background

The reliability and resilience of today's electric grid is paramount to the national security of the US. America's grid encompasses electric utility-owned distribution and transmission systems, third party-owned generation and storage, regional grid and market coordinators, and millions of enabling sensors, tools and analytical devices connected by controls and communications. As the grid rapidly evolves and becomes increasingly more complex, secure communication capabilities for both voice and data become even more critical for maintaining the integrity and reliability of the grid. Reliable grid operations depend on secure communication methods to collect and share data from millions of field devices, provide remote control of field equipment, and coordinate activities between control centers and field personnel. Resilient communications networks are also crucial to support power restoration, including in the aftermath of adversary attacks that may seek to disrupt those networks as well as grid infrastructure and operations.

Threats to American communications systems are intensifying. In particular, the Salt Typhoon campaign conducted by People's Republic of China (PRC) poses a severe and continuing challenge to the US telecommunications (telecom) systems on which many utilities rely in whole or part to support their critical functions.[1] Disruptive attacks are also occurring against the telecom systems on which US allies depend, including against Vodafone. Where private utility grade networks exist, they are engineered to meet stringent service availability, latency, cyber security, and interoperability requirements not achievable via commercial networks designed for mass market applications.

The Electricity Advisory Committee (EAC) urges the Administration to help protect the reliability of the entire electric grid by recognizing and supporting the energy sector's efforts to meet its growing need for private, secure, robust wireless broadband communications networks. While these recommendations focus specifically on the electricity sector, there are broader implications for all critical infrastructure including natural gas.

While this proposal refers to "the electric utility" for convenience, it seeks to establish a redundant, secure communications system that can be scaled to reach not only electric utilities and regional grid operators, but also non-utility bulk power system components such as wholesale generators and energy storage operators. This system might also be extended to reach distribution assets, although the initial focus is for bulk power system operators and assets. Additionally, this proposal is intended to encompass the breadth of broadband technologies, both land-based and wireless.

The Grid's Dependence on Telecom Networks

Many utilities rely on third party commercial telecom providers for much of their communication infrastructure. This can introduce undefined risks, known in industry parlance as a black box risk. Due to variations in the equipment choices, speed, quality and security practices of third-party infrastructure, reliance on third-party telecom makes it harder for electric industry participants to identify potential threats, risks, and common points of failure across these communication networks. Third party telecom providers have different commercial objectives from utilities, and their objectives and practices may conflict with utilities' critical communication needs. Utilities seek to lower their telecom risks by insulating themselves from third party black box risks, by creating and using networks that are isolated from the internet and have stronger cybersecurity protections than commercial carriers' mass market services. Hence, the electric utility industry sees the need for privately controlled, utility-owned, utility-grade communication networks.

Infrastructure owners and operators in other sectors, including the oil and natural gas subsector and the water sector, are increasingly concerned with ensuring the survivability of their networks as well.

Private, utility-grade communication networks play a vital role in ensuring reliability for the grid of the future. Utility grade networks are engineered to meet stringent service availability, latency, cyber security, and interoperability requirements that cannot typically be achieved via commercial networks designed for mass market applications. System operators also rely on a defense in-depth strategy to maintain both voice and data communication capabilities. Robust, secure communication networks for national security critical infrastructure such as the electric grid cannot rely on any single method of communication. Rather, critical infrastructure sectors should use a well-designed combination of multiple diverse communication modes – private utility broadband, private utility fiber networks and third-party telecom providers – operated and used in a redundant fashion. The utility sector needs network designs that leverage diversity and security across multiple modes while minimizing or eliminating single points of failure. Finally, these secure networks should be fully interoperable and extendable.

While System Operators go to great lengths to create redundancy in their communication systems, industry security exercises like ISAC GridEx continue to identify the need for additional focus on secure data transfer techniques and secure voice communication capabilities. The most recent GridEx identified two key communications-related recommendations: (a) the need to enhance the resilience of inter-control center data exchange capabilities, and (b) the need to employ alternate technologies for operator voice communications essential to grid operations.

Specific Challenges

Industry analysis demonstrates the cyber threat to energy industry operations is real; unclassified threat assessments, incidents and government statements prove that adversaries intend to exploit the risk. Further, a number of industry technical failures have demonstrated that operational failures due to communications can occur absent adversarial intent. Whether the threat is created by an adversary, a natural hazard, or a technical failure, it is in the interests of the utility sector, the telecommunication sector, and the Nation to address this problem.

- **Fact 1**. Electric Reliability relies directly on high reliability, high integrity telecommunications. Secure, reliable and resilient communication capability is critical for the reliable operation of the electric grid and plays a significant role in ensuring national security.

- **Fact 2.** Technical failures and natural hazards have impacted telecommunications. Heavy reliance on third party commercial providers is insufficient and introduces multiple risks.

- **Fact 3.** Public (commercial carrier) networks are designed and operated for the mass market with different (frequently less rigorous) security, reliability, and performance goals than required by electric utilities.

- **Fact 4.** The PRC and Russia have demonstrated the intent and capability to target telecommunications. Systemic risk (red team) analysis highlights how hostile telecommunications targeting could impact reliable electric operations and/or restoration. The PRC's interest in causing societal impact aligns with the systemic risk to the Bulk Electric System. This provides a call to action to address this 'black box risk' for utilities, with US Government support.

- **Fact 5.** Data demands necessary for reliable grid operations continue to grow as the grid becomes increasingly complex. More spectrum[2] will be needed eventually. While multiple utilities have found

[2] Spectrum refers to Radio Frequency (RF) spectrum and is a portion of the electromagnetic spectrum used for wireless communication. In the United States, regulatory responsibility for the radio spectrum is divided between the Federal Communication Commission (FCC) and the National Telecommunications and Information Administration (NTIA)

the currently available spectrum sufficient to meet their needs today and for years to come, an additional spectrum for utilities (already the subject of an FCC proceeding) will help. Sufficient dedicated spectrum is necessary for the reliable operation of critical electric infrastructure.

- **Fact 6**. There is no single communication technology or system that all critical infrastructure stakeholders can rely on during a black sky event. Most existing and emerging communication systems used in the energy industry depend on commercial carriers, including emergency satellite technologies. This dependency poses a significant risk to the resilience and reliability of critical infrastructure during extreme events. Therefore, any emergency communication solution or new communications networks must have low vulnerability and high resilience and be designed to interoperate with other existing emergency and normal communication systems as they are restored.[5]

Purpose and Scope

This paper focuses on near-, mid- and long-term recommendations for DOE's immediate action. The EAC's goal is to promote and facilitate the development and expansion of private utility owned communication infrastructure to enhance the overall resilience of the electric grid. In particular, these recommendations directly support the DOE Office of Electricity strategic goals under CESER and the grid modernization initiative by enhancing communications infrastructure resilience, supporting digitization, and enabling secure data flow across interconnected energy systems.

Additional Considerations

- **Spectrum:** The need for spectrum is a key communications regulatory policy issue for utilities. In the long-run, utilities will need spectrum for cybersecurity, resiliency and reliability reasons. The evolution of grid operations requires communication networks that can support AI-driven situational awareness, predictive maintenance, and dynamic load balancing. Well-structured utility-owned broadband can provide the bandwidth, control and security necessary to safely integrate these advanced technologies. The current policy dialogue is focused on freeing up spectrum for commercial auctions or for unlicensed use, but overlooks the spectrum need for other entities, particularly critical infrastructure, for licensed, exclusive use spectrum. It is very challenging, if not almost impossible, for utilities to compete successfully in auctions at prices that their customer can bear and obtain the geographic coverage that they need. Unlicensed spectrum does not offer the same reliability and operational certainty as licensed, exclusive use spectrum. And while spectrum sharing has been discussed in the past, it has not been approached in a way that first considers whether the parties sharing the spectrum have compatible needs and missions (versus whether their respective technologies can be made to somewhat co-exist)[3]. Therefore, electric utilities believe that licensed spectrum dedicated to the exclusive use of electric utilities is necessary to reduce grid vulnerability and improve grid resilience.

- **Affordability:** Utilities must balance customer cost and affordability with national security risks. Private networks offer a higher reliability than commercial networks but also come at a higher cost. Incentives may be needed to allow and encourage electric companies to enhance the resilience of their communication systems and support national security interests.

- **Commercial drivers:** Cost and commercial drivers result in the proliferation of cheap telecom components sold by companies affiliated with foreign adversaries. Even in cases where utilities intend to avoid the use of unsecure components, it can be difficult to identify the bad actors due to the use of

[3] See American Public Power Association Issue Brief regarding Protecting 6 GHz Spectrum usage by Public Power from Interference. Protecting 6 GHz Spectrum Usage by Public Power from Interference | American Public Power Association

shell corporations and shifting business relationships. Utility industry members and others need help identifying the vendors and manufacturers of telecom equipment that represent security risks; such providers should be added to the federal government's blacklisted companies.

- **Dual Benefit:** The US Department of Defense recognizes the value of private broadband as a part of our national defense strategy. The DOD Private 5G Deployment Strategy contemplates the deployment of private 5G networks at military installations and other users. As DOD emphasizes, "our world is changing, and the Department must accelerate adoption and implementation of 5G technology to deliver new levels of wireless mobility network performance, capabilities, and efficiencies that contribute to the warfighting capacity and lethality of the Joint Force."[4]

- **Interoperability:** Interoperability of the utility private broadband networks across the US is important but should be straightforward as long as utilities adopt standards-based (3GPP-based) technologies (4G and 5G). The chipsets/modules in the devices will be very important in terms of the spectrum bands that they support. A chipset/module can support many spectrum bands, but volume and device ecosystem drive which spectrum bands manufacturers include. All utilities do not have to use the same spectrum bands in their network, but they need to use a set of common, widely supported spectrum bands. Interoperability will be feasible if most utilities deploy some form of private 4G and/or 5G network on standard spectrum bands, but one-off spectrum bands will inhibit interoperability.

- **Artificial Intelligence (A) Issue**s: The evolution of grid operations requires communication networks that can support AI-driven situational awareness, predictive maintenance, and dynamic load balancing. Utility-owned broadband should provide the bandwidth, control and security necessary to safely integrate these advanced technologies.

- **FCC Considerations**
  - Utilities and DoD will eventually need access to additional dedicated spectrum.
  - Utilities and DoD networks must be free from interference, including that arising from open access to spectrum.

Recommendations

These recommendations to create robust, resilient electric system communications capabilities directly support the DOE Office of Electricity, DOE Office of Cyber Security, Energy Security and Response (CESER) strategic goals and the grid modernization initiative by enhancing communications infrastructure resilience, supporting digitization, and enabling secure data flow across interconnected energy systems.

- DOE should promote the adoption of private broadband communications technology by electric companies to enhance resilience against cyber-attacks and facilitate increased data as A.I. use expands.

- DOE should fund pilot programs and provide research grants to develop secure, private broadband networks either operated by electric utilities or operating securely over public carrier systems. Those efforts should be informed by risk assessments, security guidelines, and other initiatives led by the National Institute of Standards and Technology (NIST) on communications security, including for hardware and software supply chain validation for telecom infrastructure and critical energy applications.

- DOE should encourage the FCC to allocate licensed spectrum specifically for the use of electric utilities and draw on equivalent efforts underway by the Department of Defense in shaping strategies for the energy sector.

- GridEx exercises with the government and the electric utility industry should incorporate real-time scenarios resulting in the loss of communications along with interruptions to electric service.

- The adoption of private wireless broadband communications is also recommended for other defense-critical infrastructure industries (DCII) such as oil and gas pipelines, transportation, etc.

- DOE should develop guidance on best practices for communications network segmentation, interoperability and redundancy. In particular, as the Department of Defense develops best practices for communications network segmentation, interoperability and redundancy, DOE should leverage those efforts and adapt them to meet the specific needs and circumstances of the energy sector.

- DOE should require communications risk assessments for use with DOE-funded grid modernization or cyber resilience initiatives and private industry initiatives.

- DOE should explore infrastructure and institutional options for how to establish and maintain secure, private broadband networks controlled by members of the electric industry for the use of most of all members.

- DOE should support the development and deployment of an independent, redundant communication capability that can be utilized nationwide in the near term to address grid recovery during black sky events. This emergency communication solution must be designed to interoperate with other existing emergency and normal communication systems as they are restored, for resilience and reliability during extreme events.

Request for Administration Support

In light of the above, the Electricity Advisory Committee urges the Administration to help ensure electricity grid reliability by recognizing and supporting the energy sector's efforts to meet its growing need for private, secure, robust wireless broadband communications networks.

Citations

[1] Tim Starks, "Salt Typhoon telecom breach remarkable for its 'indiscriminate' targeting, FBI official says," Cyberscoop, February 19, 2025, https://cyberscoop.com/salt-typhoon-telecom-breach-remarkable-for-its-indiscriminate-targeting-fbi-official-says/; Matt Kapto, "Salt Typhoon remains active, hits more telecom networks via Cisco routers," Cyberscoop, February 13, 2025, https://cyberscoop.com/salt-typhoon-china-ongoing-telecom-attack-spree/; A.J. Vincens, "US adds 9th telcom to list of companies hacked by Chinese-backed Salt Typhoon cyberespionage," Reuters, December 27, 2024, https://www.reuters.com/technology/cybersecurity/us-adds-9th-telcom-list-companies-hacked-by-chinese-backed-salt-typhoon-2024-12-27/; Cybersecurity and Infrastructure Security Agency (CISA), Strengthening America's Resilience Against the PRC Cyber Threats, January 15, 2025, https://www.cisa.gov/news-events/news/strengthening-americas-resilience-against-prc-cyber-threats

[2] Portugal's network which disrupted services for several days in 2022.

[3] Vodafone Portugal hit by hackers, says no client data breach, Reuters, February 8, 2022, https://www.reuters.com/technology/vodafone-portugal-hit-by-hackers-says-no-client-data-breach-2022-02-08

[4] Department of Defense (DOD), DOD Private 5G Deployment Strategy, October 16, 2024, https://dodcio.defense.gov/Portals/0/Documents/Library/Private5GDeploymentStrategy_508.pdf

[5] EPRI "Resilient Communication Demonstration Project: Demonstration Evaluation Report" https://www.epri.com/research/products/000000003002017908