U.S. Department of Energy
Office of Electricity, Energy Resilience Division
1000 Independence Avenue, SW
Room 8H-033
Washington, DC 20585

Subject: **Ensuring the Continued Security of the United States Critical Electric Infrastructure**

To Whom It May Concern:

The Communications Sector Coordinating Council (CSCC)[1] is pleased to comment on the Request for Information (RFI) of the Department of Energy (DOE) in its proceeding[2] requesting input from stakeholders regarding measures to ensure the continued security of critical electric infrastructure. As the Department notes, electric power is vital not only to national energy security, but also to other critical infrastructure, including communications systems, and the continuity of the broader national economy.

[1] Chartered in 2005, the Communications Sector Coordinating Council (CSCC) coordinates industry engagement with the U.S. government on cyber and infrastructure security. Communications is one of sixteen Critical Infrastructure/Key Resource (CI/KR) sectors identified in the DHS National Infrastructure Protection Plan (NIPP). CSCC coordinates with industry participants in the National Security Telecommunications Advisory Committee (NSTAC) and the Communications-Information Sharing and Analysis Center (NCCIC).

[2] 86 FR 21309, Notice of Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure, https://www.federalregister.gov/documents/2021/04/22/2021-08482/notice-of-request-for-information-rfi-on-ensuring-the-continued-security-of-the-united-states

CSCC strongly supports the Department's goal to ensure electric power is reliably available across critical infrastructure, thereby ensuring communications infrastructure can continue to support a wide range of important functions without interruption, from national security and emergency services to healthcare, education, and other public necessities.

We offer the following insights based on consultation with national security and emergency preparedness (NS/EP) experts in the communications sector, with the goal of highlighting the connection between energy security and communications resilience and encouraging appropriate planning activities.

I. Development of Long-Term Strategy

CSCC supports the Department's decision to develop a long-term strategy to ensure the security of critical electric infrastructure. We believe such strategy should include opportunities for input from the broad set of relevant stakeholders across all of the energy-dependent critical infrastructure sectors, but particularly the communications sector given the co-evolution of communications and electric infrastructure, our increasing dependencies on electric power and the centrality of our services to basic functions of society.

Different sectors can contribute unique insights about how dependencies on electric power affect them, enabling the Department to prioritize rational goals and avoid generalizations that may prove less efficient than flexible and targeted solutions. The Department should also in appropriate circumstances consider input from specific industries within sectors about their unique needs. As the Department recognizes, "innovative approaches will be needed to thwart continually evolving threats."[3]

a) The long-term strategy should anticipate increased demands for electric power by communications networks and the broader ICT ecosystem.

5G networks will be up to 90% more energy efficient than legacy 4G networks due to a variety of technological advances.[4] The vastly improved energy efficiency will enable communications providers to offset to a significant extent the environmental impact of deploying

[3] *Id.* at 21311

[4] Press Release, Nokia, Nokia Confirms 5G as 90 Percent More Energy Efficient (Dec, 2, 2020) https://www.nokia.com/about-us/news/releases/2020/12/02/nokia-confirms-5g-as-90-percent-more-energy-efficient/

next-generation connectivity to communities across the United States, leading to a more sustainable future environment.

Nonetheless, as with every previous mobile generation, the deployment of 5G will increase the net requirement for energy resources. Many providers expect their energy consumption to double in the near future,[5] as they densify their networks to meet increasing traffic demands and prepare to roll out 5G frequencies to serve more communities. Providers will be faced with the challenge not only to extend geographical coverage, but also to support the explosive growth of connected devices (e.g. IoT devices) in new operating environments and increased connectivity at the sites where such devices are currently deployed. Within the next four years, mobile networks may have to carry four times the data of today's networks.[6]

As we head toward these uncharted territories, any long-term strategy for national energy security should seek to guarantee availability of energy resources for communications and broader ICT resilience. As noted by the President's National Security Telecommunications Advisory Committee (NSTAC) in the *2021 Report to the President on Communications Resiliency*,[7] "While the communications sector has extensive back-up power in place to ensure ongoing operations, not every network element lends itself to this type of protection. As the industry moves to a 5G/Next-Gen environment, it is unclear to what extent this reliance on power becomes exacerbated or mitigated, particularly given the billions of IoT devices that may be elements in critical services."[8] Although electric infrastructure is in the process of evolving toward a "Smart Grid", which includes a number of benefits to energy resiliency,[9] none of these improvements actually reduce the communications sector's reliance on electric power.

---

[5] Mats Pellbäck Scharp and Ove Persson, Why We Need a New Approach to Network Energy Efficiency at 1 (2020), https://www.ericsson.com/en/blog/2020/3/5g-network-energy-efficiency

[6] Ericsson, Ericsson Mobility Report at 13 (2020), https://www.ericsson.com/en/mobility-report

[7] The President's National Security Telecommunications Advisory Committee, NSTAC Report to the President on Communications (2021), https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Communications%20Resiliency.pdf

[8] NSTAC at 9.

[9] *Id.* ("quicker restoration of electricity after power disturbances; more efficient transmission of electricity; increased integration of large-scale renewable energy systems; better integration of customer-owner power generation systems, including renewable energy systems; and improved security").

As the Department has noted, "Although the electric grid is considered an engineering marvel, we are stretching its patchwork nature to its capacity."[10] Likewise, the NSTAC Communications Resiliency Subcommittee concluded that despite the evolution toward Smart Grid, operational dependency between ICT and electricity providers "remains critical" and the nation would benefit from forward-looking assessments to determine "how the power, IT, and communications sectors could interact to become better informed and collaborate to assure the delivery of each sector's critical functions."[11] Efforts are currently underway within the DHS National Risk Management Center (NRMC) to increase government and private sector understandings of dependency and interdependency of cross-sector critical functions. This effort and potentially others should inform the Department's strategic thinking.

b) The long-term strategy should address cybersecurity and supply chain risk management.

Consistent with the RFI, the Department's efforts may properly include an examination of supply chain risk management practices and industrial control and operational technology system security. As the Department has stated, "[a]dversarial nation-state actors are targeting our critical infrastructure, with increasing focus on the energy sector."[12] These adversaries recognize that any significant compromise of electric infrastructure poses significant risks for public welfare, in no small part because of cross-sector dependencies on the reliable supply of electric power.

As a recent GAO Report notes, the U.S. grid's distribution systems "are increasingly at risk from cyberattacks. Distribution systems are growing more vulnerable, in part because their industrial control systems increasingly allow remote access and connect to business networks. As a result, threat actors can use multiple techniques to access those systems and potentially disrupt operations."[13] The Report also notes the importance of DOE addressing distribution systems'

[10] Department of Energy, "The Smart Grid," https://www.smartgrid.gov/the_smart_grid/smart_grid.html

[11] NSTAC at 9.

[12] 86 FR 21309 at 21310.

[13] U.S. Gov't Accountability Off., GAO-21-81, Electricity Grid Cybersecurity: DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems (2021), https://www.gao.gov/assets/gao-21-81.pdf

vulnerabilities related to supply chains because without addressing supply chain issues DOE's plans would be of limited use in prioritizing federal support to states and industry.[14]

A non-exhaustive set vulnerabilities highlighted in the report includes the following:[15]

- industrial control systems increasingly include remote access capabilities to monitor and control operations and connect to corporate business networks;
- grid operations increasingly rely on global positioning systems (GPS) for critical position, navigation, and timing information; and
- more networked consumer devices and distributed energy resources, which provide increased monitoring and control capabilities for consumers and utilities, are being connected to distribution systems networks.

To address these systemic risks, CSCC believes that a coordinated national strategy that involves substantial input from the private sector, including all energy-dependent sectors of the U.S. economy, is the best path forward.

c) The long-term strategy should include plans to modernize and improve grid resilience given co-dependencies with other sectors.

CSCC offers the following policy proposals for the Department's consideration, in order to improve grid resilience and better align the energy sector with all other critical infrastructure providers that rely on energy, including the communications sector:

1) <u>Increasing the reliability and recovery capabilities in the power distribution system.</u>
    - Energy sector providers should complete assessments of and prioritize overhauls of their most vulnerable service areas.

[14] *Id*. at 31–32.

[15] *Id*. at 11.

- Energy sector providers should harden the power distribution network against known disaster scenarios that occur (including extreme prolonged heat or cold weather, earthquakes, flooding, high winds, hurricanes, tornadoes, blizzards, fires, etc.), as this would benefit all power users.
- Liberalizing or increasing empowerment of power providers and other utilities to trim trees is a simple and cost-effective practice to that benefits power providers as well as all power users.

2) Enhance information sharing for the Energy Sector to keep Critical Infrastructure Providers and the general public better informed of outages and restoral efforts.
   - Relevant authorities should consider incentives for the providers in the energy sector and other critical infrastructure providers to develop a mutual aid agreement that facilitates information sharing and mutually beneficial aid during times of significant power outages and other emergencies.
   - Advance notification by power providers of planned blackouts and disclosure of critical points of potential weakness or risks would be extremely useful to critical infrastructure providers, allowing such providers to prepare in advance by pre-staging and allocating resources optimally.
   - Increased information sharing by the energy sector could include power distribution companies communicating where power outages occur, where power companies are restoring service first, and the sequence of major restoration efforts, all of which would be helpful in staging and optimizing disaster response activities of other critical infrastructure providers.
   - Similarly, transparency with the public regarding planned outages would allow the general public (individuals and small businesses) to prepare and make alternative arrangements.

3) Designate Critical Infrastructure Providers, such as Communications Sector Providers, for Priority Electric Service Restoration.
   - Criteria should be established to identify entities that qualify for prioritized power restoration. As an example, the Communications Sector currently use the

Telecommunications Service Priority (TSP) program managed by the Department of Homeland Security (DHS) and the energy sector could implement a program similar to the TSP program.

- Notably, to be effective, a prioritized power restoral designation must be limited to critical infrastructure providers (i.e., if everyone is prioritized, no one is prioritized).

II. Conclusion

CSCC appreciates the opportunity to raise awareness of how communications resiliency depends on electric power, and therefore could be impacted by the Department's strategy. As the Department takes steps to develop a long-term strategy that ensures the continued resilience of electric infrastructure, including against cybersecurity and supply chain attacks, we stand ready to engage in these discussions as interested stakeholders and willing partners.

Respectfully Submitted,

/s/ Paul Eisler

Paul Eisler
Senior Director, Cybersecurity
USTelecom – The Broadband Association
601 New Jersey Avenue, NW, Suite 600
Washington, DC 20001
(202) 326-7300

June 7, 2021