Written Testimony of the Honorable Bruce J. Walker JD

President & Chief Executive Officer

Alliance for Critical Infrastructure Security, Inc. a not-for-profit corporation

Before the United States House of Representatives

Committee on Energy and Commerce

Subcommittee on Oversight and Investigations

July 18, 2023

Chair Griffith, Ranking Member Castor, and distinguished Members of the Subcommittee, I appreciate the opportunity to submit testimony regarding existing and emerging threats to the electric grid. My name is Bruce Walker, and I am the former United States Senate confirmed Assistant Secretary for the Office of Electricity at the United States Department of Energy. Today, I am President & CEO of the nonprofit Alliance for Critical Infrastructure Security (ACIS). ACIS's key mission is to facilitate the collaboration between critical infrastructure stakeholders including asset owners and operators, trade groups, regulators, and government agencies, to identify cyber and physical risk and vulnerabilities and develop solutions to improve the security of the nation's critical infrastructure. While ACIS analyzes cyber and physical risk for all the critical infrastructure sectors, because of the reliance of all other sectors on the electric grid, ACIS places significant emphasis on the electric grid.

There are numerous existing and emerging threats to the electric system. These include challenges associated with cyber and physical threat, localized electromagnetic pulse threats, supply chain compromises by nation state actors, supply chain constraints of both large power and distribution transformers, weather related threats including wildfires, severe droughts, solar flares and extreme weather events, and the transformation of the electric grid from a unidirectional to a multi-directional power flow grid with a focus on de-centralization and decarbonization. The transformation of the electric grid, including – the integration of an unprecedented capacity of Distributed Energy Resources (DERs) in an equally unprecedented short window of time, will require careful control systems engineering and

integration to maintain the existing stability and reliability of the electric grid. The accelerating de-carbonization and retirement of coal generation is forcing the United States toward an electric generation fleet reliant upon natural gas pipelines - further increasing the electric sector's cyber and physical attack surface area.

Many of these challenges, though complex, are solvable and most already have highly capable specialized and focused organizations developing solutions and mitigations. The Electricity Subsector Coordinating Council in partnership with the electric sector trade organizations: Edison Electric Institute, American Public Power Association and National Rural Electric Cooperative Association, working alongside their membership, established a Tiger Team to address the distribution transformer shortages and other supply chain issues. Through the electric Sector's Risk Management Agency, the Department of Energy's (DOE) Office of Cybersecurity, Energy Security and Emergency Response (CESER) in conjunction with several National Laboratories[1] are developing capabilities for industry and government to sit side-by-side through the Energy Threat Analysis Center (ETAC). They are also developing modeling capabilities to facilitate the integration of renewables and improving predictive and mitigation capabilities for wildfires. Additionally, CESER, industry and Lawrence Livermore National Lab developed a threat informed systemic electric sector risk register, and Pacific Northwest National Lab's continued work focused on the expansion of capabilities in the Grid Storage Launchpad, will yield capabilities in the megawatt storage technology arena that will help better facilitate the energy transformation. Similarly, DOE undertakes significant and meaningful work with the Electric Power Research Institute in areas of reliability, resilience and grid flexibility that are helping address the challenges and the electric grid transformation.

Though the electric grid remains challenged by various risks, the most significant evolving risk is associated with cyber security, especially through communication pathways and physical security.

[1] Lawrence Livermore National Lab, Pacific Northwest National Lab, Sandia National Lab, Oak Ridge National Lab, Idaho National Lab, Argonne National Lab and National Renewable Energy Lab

The United States electric grid is one of the most complex and important machines in the world. All of society is dependent upon its unwavering reliability and our adversaries are keenly aware of our reliance on the electric grid.

As noted in the 2023 Annual Threat Assessment of the Intelligence Community (IC),[2]

"China's cyber espionage operations have included compromising telecommunications firms, providers of managed services and broadly used software, and other targets potentially rich in follow-on opportunities for intelligence collection, attack, or influence operations." In that same report, the Office of the Director National Intelligence (ODNI) notes, "China almost certainly is capable of launching cyber-attacks that could disrupt critical infrastructure services within the United States, including against oil and gas pipelines, and rail systems." This is particularly troubling and pertinent to emerging risks as we are significantly reliant on gas transmission pipelines for electric generation – in fact, on July 14, 2023 gas fired electric generation was 45% across the continental United States with two regions exceeding 66%.[3] The United States reliance on gas fired electric generation is only increasing as government policies and investment move the industry away from other fossil fuel generation.

The threat does not come from China alone. In addition, "Russia is particularly focused on improving its ability to target critical infrastructure, including underwater cables and industrial control systems, in the United States as well as in allied and partner countries, because compromising such infrastructure improves and demonstrates its ability to damage infrastructure during a crisis."[4]

The cyber risk is further complicated by political instability which increases the possibility of a potential miscalculation and associated escalation created by the on-going war in Ukraine – as noted in the 2023 Annual Threat Assessment of the Intelligence Community:

[2] 2023 Annual Assessment of the Intelligence Committee, Submitted by the Office of the Director of National Intelligence to Congress on February 6th, 2023, page 10.
[3] Real-time Operating Grid - U.S. Energy Information Administration (EIA)
[4] 2023 Annual Assessment of the Intelligence Committee, Submitted by the Office of the Director of National Intelligence to Congress on February 6th, 2023, page 15.

"Russia's unprovoked war of aggression against Ukraine is a tectonic event that is reshaping Russia's relationships with the West and China, and more broadly in ways that are unfolding and remain highly uncertain. Escalation of the conflict to a military confrontation between Russia and the West carries the greater risk, which the world has not faced in decades."[5]

Importantly, the risk associated with cyber is exacerbated by the rapid transformational changes happening in the electric sector. The transition away from a centralized generation and command and control model to a decentralized model, has increased the surface area for cyber penetration. Specifically, DERs often rely on cloud service technology and / or commercially available communication platforms for aggregation services for command and control of their systems. As noted by the Department of Energy's Office of Electricity, "the controllability of DER assets is fundamentally different from that of centralized generation due to the former's geographically dispersed nature… resulting in a heavy reliance on communications for remote control and monitoring (and very likely the internet)."[6] Further, both cloud technologies and commercially available communication platforms are rich targets for executing cyber-attacks.

Similarly, many utilities throughout the United States rely upon commercially available communications for command and control of their systems. Compromised communications can provide access to both Information Technology (IT) and Operational Technology (OT). Although the vulnerabilities in IT systems are well known, the threat now focuses and is increased on the exploitation of vulnerabilities of energy delivery systems via OT.[7] OT systems consist of industrial control systems, programmable logic controls, and their associated supervisory control and data acquisition software. The heavy use of OT systems has made electric utilities, oil and natural gas providers, hydro and nuclear facilities, railway, ports, and water utilities prime targets for OT-related cyber-attacks. The disruption of

[5] 2023 Annual Assessment of the Intelligence Committee, Submitted by the Office of the Director of National Intelligence to Congress on February 6th, 2023, page 12.
[6] Department of Energy, Office of Electricity - Communications in the Electric Grid: An Evolving Interdependent Ecosystem between the Grid and Communications Utilities; page. 4. Communications in the Electric Grid: An Evolving Interdependent (energy.gov)
[7] Department of Homeland Security – Cybersecurity Infrastructure Security Agency Industrial Control Systems | Cybersecurity and Infrastructure Security Agency CISA

any one of these critical infrastructure sectors is not only inherently problematic for societal needs but, it also hampers the United States' ability to sustain the economic and military strength needed to protect our country and maintain our way of life.

Recent efforts to address IT/OT threats includes the Federal Communications Commission (FCC) establishment of a Supply Chain Reimbursement Program (SCRP) with Congressionally supported funding set at $1.9bn to remove communication equipment and services produced or provided by Huawei Technologies Company or ZTE Corporation. This was the result of the United States government's determination that use of communication devices from these Chinese companies posed a national security threat. It should be noted that when SCRP - *which was only available to advanced communication providers with ten million or fewer customers* - was established, it was quickly oversubscribed; and the FCC received applications seeking more than $5.6bn.

In addition to the cyber threat already discussed herein, physical threats pose a significant risk to the electric grid. In fact, "physical attacks on the U.S. power grid rose by 71% in 2022 compared with 2021, according to an industry analysis conducted by the North American Electric Reliability Corporation's (NERC) Electricity Information Sharing and Analysis Center, which shows that ballistic damage, intrusion, and vandalism largely drove the increase in physical attacks on the power grid."[8]

Since the Metcalf incident in April of 2013, industry spent considerable funding hardening the grid. In 2014 the Federal Energy Regulatory Commission, informed by NERC, adopted Critical Infrastructure Protection Standard 14 (CIP-14) to improve the security of certain Bulk Power System assets. Recent events in North Carolina and Washington demonstrate there is more to do. Domestic Violent Extremist groups focus on the electric grid also increases the risk of physical threat.[9] Industry

[8] U.S. power grid physical attacks rose by 71% in 2022, E-ISAC Report Finds, posed on February 21, 2023, by Frisch report.
[9] North American Electric Reliability Corporation, 2023 State of Reliability Overview, available at https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_SOR_2023_Overview.pdf

working in partnership with the FBI, DOE, DHS and others, must continue to stay vigilant against this physical threat.

In addition to already realized physical threats, there are other threats, including drone technology which can be weaponized against the electric grid. Further, information regarding physical threat scenarios is included by the Department of Homeland Security, Cybersecurity Infrastructure Security Agency in their Publication on Physical Security Scenarios - Active shooters, vehicle ramming, improvised explosive devices (IEDs), unmanned aircraft systems (UASs), and many more.[10]

Neither the cyber nor physical threats that the United States electric grid is facing can be fully addressed through industry efforts and federal government partnerships as they exist today. To successfully protect critical infrastructure in today's current and emerging threat environment, we must approach this problem differently than we have in the past – we must transition to an all-of-society approach – an approach that utilizes appropriate federal capabilities to protect critical infrastructure assets; especially, the electric grid. Over the past decades, critical infrastructure asset owners did not build their systems to defend against nation state adversaries and Domestic Violent Extremists – protection against these threats was the role of the federal government.

The Alliance for Critical Infrastructure Security was formed to mitigate the risks being faced by critical infrastructure, especially the electric grid, to protect the American way of life. Together, through an alliance of government and industry, the grid can remain secure into the future.

Thank you for the opportunity to provide testimony for this important topic and I look forward to any questions you may have.

Bruce J. Walker

[10] Physical Security Scenarios | CISA