Testimony of

CAITLIN DURKOVICH

Director, Toffler Associates

Former Assistant Secretary, Infrastructure Protection,
National Programs and Protection Directorate
Department of Homeland Security

Submitted to the

SENATE HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS COMMITTEE

For the February 27, 2019 Hearing

"Perspectives on Protecting the Electric Grid from an Electromagnetic Pulse or Geomagnetic Disturbance."

Chairman Johnson, Ranking Member Peters, and members of the Committee, thank you for inviting me to testify at the roundtable today, "Perspectives on Protecting the Electric Grid from an Electromagnetic Pulse or Geomagnetic Disturbance."

My name is Caitlin Durkovich. I had the honor of serving eight years at the Department of Homeland Security (DHS) from 2009-2017, including as the Assistant Secretary of Infrastructure Protection. I also had the privilege of co-chairing the Space Weather Operations, Research and Mitigation (SWORM) Task Force, which produced *The National Space Weather Strategy* (2016) and corresponding action plan to enhance the preparedness of the Nation to a space weather event.

I now lead the security and resilience practice for Toffler Associates, a future-focused strategic advisory firm, whose clients include critical infrastructure owners and operators and the department and agencies charged with helping them manage risk in increasingly complex and uncertain times.

There is no doubt the risk facing owners and operators of critical infrastructure has increased. We are reliant on aging infrastructures built for a different time that increasingly leverage data and technology to enable more efficient, reliable and distributed operations. This highly interconnected, electrified and digitized ecosystem is not only being used for purposes we could have never imagined when it was built 100 years ago, but it must be resilient to risks we could have never imagined – extreme weather, coordinated cyberattacks, reliance on GPS, electromagnetic pulse (EMP), and severe geomagnetic disturbances (GMD) or space weather, to name a few.

These risks – and our vulnerabilities to them – transcend geographic borders, corporate lines of business, and politics, blurring the lines between public and private accountability and responsibility. It is the private sector, which owns and operates most of our critical infrastructure, that must invest in and manage the risks and often intertwined consequences posed by the threat environment.

The energy sector in particular faces a variety of threats and hazards, largely driven by the increasing sophisticated threat actors with intent and capability as well as the interdependencies of the infrastructure systems, including the increasing reliance on digital infrastructure as the electric grid transitions from an analog system to a digital system to improve efficiency. The bottom line is the risk to digital and physical infrastructures has grown and our critical infrastructure is more vulnerable than it was a few decades ago.

What is encouraging is the partnership between government and industry has matured, providing more visibility into emergent threat vectors and potential consequences – guiding joint action on risk mitigation. We must continue to support and incentivize owners and operators to understand and protect infrastructure not just from the routine, but from the most consequential and disruptive threats – terrestrial and space-based – that pose existential risk.

The challenge we face is sustained focus and engagement on the lower probability, high consequence threats that are overshadowed by high likelihood, real-time threats that require regular, and sometimes 24x7 hour attention, such as cyberattacks.

Potential Impacts to Critical Infrastructure from EMP on GMD

We do not fully understand how an EMP event or space weather event would impact electrical infrastructure, and it is the subject of ongoing analysis. In some of its forms, EMP and

GMD could cause widespread disruption and serious damage to electronic devices and networks, including those upon which many critical infrastructures rely. There is uncertainty over the magnitude and duration of an electric power outage that may result from an EMP event due to ambiguity regarding the actual damage to electric power assets from an event. Any electric power outage resulting from an EMP event would ultimately depend upon several unknown factors and effects to assets that are challenging to accurately model, making it difficult to provide high-specificity information to electric system planners and system operators. These variables include characteristics such as the EMP device type, the location of the blast, the height of the blast, the yield of the blast, and design and operating parameters of the electric power system subject to the blast. Secondary effects of EMP may harm people through induced fires, electric shocks, and disruptions of transportation and critical support systems, such as those at hospitals or sites like nuclear power plants and chemical facilities.

And while space weather phenomena are relatively well understood within the scientific community, the rarity of extreme space weather over the lifespan of our modern-day infrastructure has limited the availability of data useful for predictive analysis. One of the earliest recorded and most infamous geomagnetic storms – the 1859 Carrington Event – caused telegraph systems to fail across North America and Europe. A 1921 extreme GMD, similar to the 1859 Carrington event, also disrupted communication systems in the United States and Europe.

March 1940 is the earliest reported instance of GMD affecting the electric grid. The 1989 Quebec Blackout led to the interruption of power in Québec, Canada for nearly nine hours and demonstrated the potential of GMDs to cascade impacts across geographic regions. In addition to causing the Hydro-Quebec power grid to collapse in less than two minutes, the storm's arrival damaged transformers and caused tripping of protective equipment in the Northeastern United States. The Quebec Blackout is one of four storms that had consequential impacts to the grid: A September 1989 Storm cause thermal damage to North American transformers; a November 2001 storm resulted in transformer failures in New Zealand; and, the October 2003 Halloween event resulted in minor power grid disturbances in North America.

In July of 2012, a major disruptive solar event narrowly missed the earth. It would have been comparable to the 1859 Carrington event and it is believed if the storm had occurred one week earlier, earth would have been in the line of fire. Most newspapers never mentioned the near miss and I would be hard pressed to say most infrastructure operators or Americans know about the phenomena of space weather, much less can name these four modern-day space weather events or the near miss.

In the development of *The National Space Weather Strategy*, the SWORM Task Force also recognized that the growing interdependencies of critical infrastructure systems have increased potential vulnerabilities to EMPs and GMDs and other lower probability, high impact events. Cross sector protection and mitigation efforts to eliminate or reduce EMP and GMD vulnerabilities are essential components of national preparedness. Protection focuses on capabilities and actions to eliminate vulnerabilities to EMP and GMD, and mitigation focuses on long-term vulnerability reduction and enhancing resilience to disasters. Together, these preparedness missions frame a national effort to reduce vulnerabilities and manage risks associated with EMPs, GMDs, and other unbounded events.

Government and Industry Collaboration

More than two decades of critical infrastructure programs and policies has fostered unprecedented collaboration between government and industry to mitigate the consequences of low probability, high consequence events, including EMP and GMD. I want to applaud the Department of Homeland Security for its releasing its strategy for *Protecting and Preparing the Homeland Against Threats of Electromagnetic Pulse and Geomagnetic Disturbances*. The strategy's three goals are practical steps the critical infrastructure enterprise can coalesce around to mitigate the risk of EMP and GMD. They include:

1. Improve risk awareness of electromagnetic threats and hazards.
2. Promote effective electromagnetic-incident response and recovery efforts.
3. Promote effective electromagnetic-incident response and recovery efforts.

I agree with the Department's assessment about the potential severity of both the direct and indirect impacts of an EMP or GMD incident, and that it should compel our sustained national attention. Taking a page from hurricane preparedness, the SWORM Task Force went to great lengths to understand how much advance warning owners and operators need to put effective mitigation measures in place. This information was the basis for improving forecasting lead-time and accuracy and ensuring that products are actionable for decision making. However, if the community is unaware of this environmental hazard, or has not institutionalized it as part of contingency planning and operations, better forecasting will have little effect. One of the biggest challenges I believe EMP and especially GMD risk mitigation faces, is sustained focus on this hard problem. Efforts to to raise critical infrastructure stakeholder understanding of space weather in an increasingly chaotic risk environment are critical. I want to thank the Ranking Member for continuing to advance legislation to improve the understanding and forecasting of space weather events and ensure the homeland security enterprise better understands the vulnerability of critical infrastructure to space weather events. I also believe this is where we can take another page from hurricane preparedness and ensure key stakeholders partake in annual space weather briefings and planning conferences.

Finally, I support the objective of developing effective public risk communication plans to promote consistent messaging and addressing public uncertainty. Many of the EMP and GMD mitigation measures would result in a disruption to the lifeline functions our public takes for granted. However, if the risk is better understood, the public can play an important role in helping us limit the damage and disruption.

Conclusion

EMP and space weather are two of the many threats to the functions, systems, and networks that underpin our national security, economic prosperity, and American way of life. From cyber espionage and sabotage, to the convergence of cyber and physical systems, to insider threats, and to EMPs and GMDs, owners and operators of critical infrastructure have an obligation to manage threats across the risk spectrum – routine, persistent, and existential – but should not have to go it alone. These challenges demand industry and government work together to both develop mitigation strategies and to invest in a modern and secure infrastructure that is resilient to the threats of today and tomorrow.

Chairman Johnson, Ranking Member Peters, and members of the Committee, thank you again for the opportunity to appear before you today. I look forward to your questions.