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 ENERGY & NATURAL RESOURCES COMMITTEE

For the May 4, 2017 Hearing

"To Examine the Threat Posed by Electromagnetic Pulse and Policy Options to Protect Energy Infrastructure"

Chairman Murkowski, Ranking Member Cantwell, and members of the Committee, thank you for inviting me to testify at the hearing today, "To examine the threat posed by electromagnetic pulse and policy options to protect energy infrastructure and to improve capabilities for adequate system restoration."

My name is Caitlin Durkovich. I had the honor of serving eight years in the National Protection and Programs Directorate at the Department of Homeland Security (DHS), first as the Chief of Staff and from May of 2012 to January 2017, as the Assistant Secretary of Infrastructure Protection. NPPD leads the national effort to protect and enhance the resilience of the nation's physical and cyber infrastructure.

I have transitioned from government to Toffler Associates, a future-focused strategic advisory firm that architects better futures for public and private sector clients around the globe with an unwavering commitment to be the catalyst for change.

Over my nearly twenty-year career in homeland security, I have seen critical infrastructure public-private risk management redefined to address emerging, complex issues from lone offenders to complex mass attacks, cybersecurity grid and GPS resilience, interdependencies, electromagnetic pulse (EMP) and severe geomagnetic disturbances (GMDs), and security-by-design. I have co-chaired several interagency task forces that have integrated the private sector into government strategies, including those that are most relevant today – the *Joint US-Canada*

Strategy for Electric Grid Security and Resilience (December 2016) and *The National Space Weather Strategy* (October 2015).

There is no doubt we live in a dangerous world. State and non-state actors, cyber threats, unbounded disasters, lone offenders, insiders, and promulgators of disinformation are growing in kind and consequence. These threats – and our vulnerabilities to them – transcend political treaties, geographic borders, and corporate lines of business, 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 an increasingly dynamic 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.

My colleagues in government have testified before other committees about how the public-private partnership views EMP, and my time out of government has not changed my understanding of the threat or my perspective; therefore, I will leverage the work of DHS and my colleagues within the DHS Office of Cyber and infrastructure Analysis.

Background on EMP

An EMP is the burst of electromagnetic radiation created, for instance, when a nuclear weapon is detonated or when a non-nuclear EMP weapon is used. EMPs can be high frequency, similar to a flash of lightning, or low frequency, similar to an aurora-induced phenomenon. The consequences of an EMP can range from permanent physical damage to temporary system disruptions, and can result in fires, electric shocks to people and equipment, and critical service outages.

There are two general classes of EMP of concern: (1) Nuclear sources of EMP, such as High altitude EMP (HEMP), and (2) Non-Nuclear sources of EMP (NNEP). HEMP results from a nuclear detonation typically occurring 15 or more miles above the Earth's surface. The extent of HEMP effects depends on several factors including the altitude of the detonation, the weapon yield, and whether it was designed for EMP effects. On the ground, effects may be diminished by the electromagnetic shielding, or "hardening," of assets. A high-altitude burst could blanket

the entire continental United States and cause widespread impacts to multiple sectors, including to lifeline sectors, such as the energy and communications. HEMP threat vectors can originate from a missile, such as a sea-launched ballistic missile; a satellite asset; or a relatively low-cost balloon-borne vehicle.

Non-Nuclear EMP (NNEP) can be created by sources, such as Radio Frequency Weapons or Intentional Electromagnetic Interference devices, which are designed to produce sufficient electromagnetic energy to burn out or disrupt electronic components, systems, and networks. NNEP devices can be either electrically-driven, where they create narrowband or wideband microwaves, or explosively-driven, where an explosive is used to compress a magnetic field to generate the pulse. The range of an NNEP is short (typically less than 1 kilometer) and Faraday casings with line filters and surge arresters can mitigate much of the EMP effects.

Potential Impacts to Critical Infrastructure from EMP

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

In the development of *The National Space Weather Strategy*, we recognized that the growing interdependencies of critical infrastructure systems have increased potential vulnerabilities to EMPs and GMDs. 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 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 and 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.

DHS continues to devote resources to address EMP risks, largely in three areas (1) risk assessment and analysis, (2) communication and coordination of threat information, and (3) research and development to mitigate EMP risks. NPPD, the Federal Emergency Management Agency, and the Science and Technology Directorate are working with the critical infrastructure community to ensure it has information to make critical decisions, and can respond to, assist recovery and mitigate the consequences of a potential EMP attack.

My fellow witnesses will testify to the scope of efforts industry is undertaking to continue to improve grid resilience to all-hazards. They range from continued research and development, mutual assistance and spare parts programs, supplemental operating strategies, and full-scale cross sector exercises.

Critical Infrastructure Risk Management

It is important to emphasize, however, that critical infrastructure, including the electric sector, takes a holistic approach to assessing and mitigating risks from not only EMP, but from cyber attacks, physical sabotage, and natural disasters, all of which can result in disruptions to their operations. The partnership between industry and government, which includes information sharing, capability development, training and exercises, and interoperable plans, is even more essential as our Nation continues to face an increasingly complex threat environment.

Conclusion and Recommendations

EMP is one of 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 these persistent threats. However, the solution requires a whole of community effort that is focused not on one threat but on a broad range of threats. These challenges demand industry and government work

together to both develop mitigation plans and to invest in a modern and secure infrastructure that is resilient to the threats of today and tomorrow.

You can help by continuing to support national programs that strengthen public-private collaboration and enable the critical infrastructure community to efficiently and effectively manage the complex risk environment, and by continuing to advocate for a secure and resilient critical infrastructure.

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