TESTIMONY

OF

CAITLIN DURKOVICH
ASSISTANT SECRETARY FOR INFRASTRUCTURE PROTECTION
NATIONAL PROTECTION AND PROGRAMS DIRECTORATE
U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE
THE

COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE
SUBCOMMITTEE ON ECONOMIC DEVELOPMENT, PUBLIC BUILDINGS AND EMERGENCY MANAGEMENT

U.S. HOUSE OF REPRESENTATIVES
WASHINGTON, D.C.

"BLACKOUT! ARE WE PREPARED TO MANAGE THE AFTERMATH OF A CYBER-ATTACK OR OTHER FAILURE OF THE ELECTRICAL GRID?"

April 14, 2016

Introduction

Chairman Barletta, Ranking Member Carson and Members of this Subcommittee, good afternoon. My name is Caitlin Durkovich and I am the Assistant Secretary for Infrastructure Protection within the National Protection and Programs Directorate (NPPD). Thank you for the opportunity to discuss how the NPPD fulfills its responsibility to support the Federal government's response to and recovery from all-hazards events, including the physical impacts of cyber incidents.

NPPD carries out the Department's cyber and infrastructure protection mission by leading the national effort to secure and enhance the resilience of the Nation's infrastructure. To carry out this mission, the Office of Infrastructure Protection leads and coordinates national programs and policies, and established strong partnerships across government and the private sector. We conduct and facilitate vulnerability and consequence assessments to help critical infrastructure owners and operators and State, local, tribal, and territorial partners understand and address risks. We provide information on emerging threats and hazards so that appropriate actions can be taken. We offer tools and training to our partners to help them manage the risks to their assets, systems, and networks.[1]

The partnerships and coordination structures we maintain and support during steady state conditions—before incidents occur—set the stage for the way we execute our responsibilities following an incident. To that end, my testimony today will provide you with an overview of the work that NPPD conducts to promote and maintain sector coordination structures, characterize national level risks to infrastructure (in particular the electric grid), and support response efforts in the event of an incident.

A robust, secure, and resilient energy infrastructure is essential to serving the needs of today's society, protecting public health and safety, economic security, and national security. U.S. infrastructure by its very nature supports communities with constantly evolving requirements. The electricity sub-sector in particular is currently facing a variety of threats and hazards, including malicious cyber activity, physical attacks, aging infrastructure, equipment failure, and extreme weather-related events.

A targeted cyber incident—either alone or combined with a physical attack—on the power system could lead to huge costs and cascading effects, with sustained outages over large portions of the electric grid and prolonged disruptions in communications, water and wastewater treatment services, health care delivery, financial services, and transportation. For example, the results of a 2015 Lloyds of London study suggested that a widespread cyber-attack on the Northeastern region of the United States, i.e., damaging 50 generators (approximately seven

[1] NPPD carries out its private sector engagement under and through authority delegated to the Directorate by the DHS Secretary, which includes but is not limited to: 6 U.S.C. §§ 121(d)(5), 121(d)(6), 121(d)(8), and 121(d)(10).

percent) could trigger a scenario where 93 million people are without power and the impact on the U.S. economy could range from $243 billion to $544 billion, or around a trillion dollars in the most extreme scenario (where 14 percent of the generators are damaged).[2]

Coordination Structures and Voluntary Partnerships

Since DHS was formed in 2003, we have been working with private sector partners to help them build the Nation's resilience to all types of threats. Under the National Infrastructure Protection Plan (NIPP), DHS is the lead, or co-lead, for ten of the 16 infrastructure sectors. In addition, the Office of Infrastructure Protection (IP) provides cross sector collaboration and coordination functions across all the 16 sectors by sharing information, conducting assessments of critical assets, and engaging in joint planning and exercises in order to support a national understanding of physical and cyber risks. This includes working in close partnership with the Department of Energy regarding the security of the electric grid.

Most of the Department's work with owners and operators is voluntary and the successful execution of the critical infrastructure mission relies on strong voluntary collaboration with the private sector. One key approach is to ensure that information about threats is communicated quickly to owners and operators. Through our work, DHS participates in joint Federal Government/Private Sector information sharing designed to ensure that our partners understand how disruptions and attacks on infrastructure can impact homeland security, community resilience, and our economy, and take informed action to mitigate those risks.

Industry Partnerships

Sector Councils

The partnership approach is driven by work conducted with the critical infrastructure councils, including the Electricity Subsector Coordinating Council (ESCC). The ESCC includes Chief Executive Officers (CEOs) representing each segment of the electric power industry, as well as heads of the major industry trade associations related to the Subsector. A major priority of the partnership is unifying industry and government efforts to plan and prepare coordinated responses to incidents of national significance—whether physical or cyber. The ESCC and government meetings, which take place three times a year, provide a venue to discuss national-level responses to major incidents, physical security and cybersecurity, grid resilience, and progress made on joint industry/government initiatives. These meetings are made possible by the Critical Infrastructure Partnership Advisory Council (CIPAC), an authority which allows government to engage in discussions about joint critical infrastructure planning, coordination, implementation, and operational issues, along with other relevant matters.

[2] Lloyd's and the University of Cambridge Centre for Risk Studies, *Business Blackout: The insurance implications of a cyber attack on the US power grid*, Emerging Risk Report 2015, innovation series (London, UK: 2015). The report also noted that while the scenario was improbable, it is technologically possible.

DHS and the Department of Energy (DOE), which serves as the Energy Sector-Specific Agency (SSA), collaborate with other interagency partners to provide classified threat briefings to CEOs on physical and cyber threats.

Meetings with the ESCC enable industry and government to share perspectives, identify joint priorities, and track progress. Projects conducted through this partnership include:

- The Electricity Substation Security Awareness Campaign: A 2013-2014 campaign conducted in close collaboration and coordination with DOE, the Department of Justice's Federal Bureau of Investigation (FBI), the North American Electric Reliability Corporation (NERC), the Federal Energy Regulatory Commission (FERC), and multiple industry partners. Taking place in ten U.S. and three Canadian cities, it increased awareness of the evolving risk environment and promoted increased collaboration on risk mitigation strategies, protective measures, and industry best practices.
- The ESCC Playbook: The Playbook is a crisis management framework to enable senior executives from industry and government to coordinate effectively on response and recovery matters. Following GridEx II, the ESCC developed the Playbook for responding to a National-level incident that disrupts the electric grid. The framework ensures senior government and industry executives are communicating and are available to support response and recovery efforts. By opening and formalizing these lines of communication, the industry and government can better coordinate efforts to protect the electric grid and recover from incidents as quickly as possible. The Playbook was tested through tabletop exercises with the ESCC and their staff. It was tested again as part of GridEx III.
- Cross-sector coordination: DHS and DOE work with the ESCC on efforts to institutionalize coordination with other sectors (e.g. telecommunications and transportation dependencies and interdependencies).

Assessing Infrastructure Security and Managing Infrastructure Risk

Risks, in particular grid related risks, do not conform to traditional boundaries of domain, sector, or geography. This makes the work that IP does in assessing interdependencies and larger scale vulnerabilities and consequences all the more important for gaining a full picture of risk, and informing risk decisions before, during, and after an incident.

Analyzing Interdependencies and Cascading Effects

Through our Protective Security Advisors (PSAs) located across the country, we offer critical infrastructure partners hands on assistance with vulnerability and security assessments like the Regional Resiliency Assessment Program (RRAP). The RRAP is an IP-led assessment of specific critical infrastructure and regional analysis of the surrounding infrastructure to examine vulnerabilities, threats, and potential consequences from an all-hazards perspective. The assessment identifies dependencies, interdependencies, cascading effects, resiliency

characteristics, and gaps. Energy is one of the primary focuses of a number of RRAP projects, and the dependence of other infrastructure sectors on energy, especially electric power, is regularly examined during the course of other projects. Since 2014, several RRAP projects included an assessment of security, resilience, and criticality of Business Systems, Industrial Control Systems (ICS), and Supervisory Control and Data Acquisition (SCADA) systems that provide a key service or function within a broader community or system of critical infrastructure.

Conducting the RRAP projects in the Energy Sector helps mitigate high-risk single points of failure and the lack of redundancy across systems, improve emergency response capabilities, and identify critical supply chain vulnerabilities. One example of a successful RRAP is a 2016 Region I Energy project that focuses on electric power substations with large power transformers and their resilience to extreme weather events. Based on recommendations and findings from the Quadrennial Energy Review conducted by DOE, the RRAP project will identify large power transformers in substations across Region I, assess their vulnerabilities, and provide data to decision makers who might better focus resources to protect the most vulnerable assets.

In addition to the RRAP Program, IP conducts site assistance visits and voluntary inspections using the Infrastructure Support Tool (IST). The IST makes use of a threat agnostic, model based risk analysis methodology, allowing owners and operators of critical infrastructure to apply the results of an IST inspection to a multitude of threat and hazard scenarios, informing their decisions about buying down risk.

National Response and Infrastructure Systems

The response to a major disaster or attack resulting in a failure of the electrical grid would require a nationwide effort, drawing on the catastrophic planning frameworks that make up the National Preparedness System. Such a response effort also requires the support of steady-state coordination structures established under the NIPP. NPPD supports FEMA and our interagency and whole community partners in strengthening the connection between the National Preparedness System and the partnership structures established under the National Infrastructure Protection Plan.

The coordination structures maintained under the NIPP provide a mechanism for cross-sector, coordinated information support for both situational awareness and planning efforts during response. Information requests and the development of incident-specific analysis contribute to the assessment, prioritization, restoration, and protection of infrastructure systems.

As the infrastructure coordination element of the National Operations Center (NOC), the National Infrastructure Coordinating Center (NICC) receives situational, operational, and incident-related information regarding the status of the Nation’s critical infrastructure sectors during incidents and collects input from every SSA that is consolidated into comprehensive reporting.

Sharing Information Quickly and Efficiently

Information sharing is a key part of NPPD's mission to create shared situational awareness of infrastructure impacts and vulnerabilities. NPPD, through its National Cybersecurity and Communications Integration Center (NCCIC), actively collaborates with public and private sector partners every day to make sure they have the information and tools they need to protect the systems we all rely on and continues to monitor the situation closely.

During a cyber or communications incident, the NCCIC is able to coordinate with State, local, and private sector partners as well as its own incident response entities and Federal partners, including law enforcement and the intelligence community so that the full capabilities of the Federal Government can be brought to bear in a coordinated manner. As the Federal Government's 24/7 hub for cybersecurity information sharing, incident response, and coordination, the NCCIC is critical in our efforts to ensure our nation's cybersecurity.

ICS-CERT

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) is a response component of the NCCIC, which responds to cyber incidents, vulnerabilities, and threats that can impact industrial control systems which operate critical infrastructure across the United States. In responding to cyber incidents, the ICS-CERT coordinates with law enforcement agencies; the intelligence community; Federal and SLTT governments; and control systems owners, operators, and vendors to reduce risk to the nation's critical infrastructure. The ICS-CERT team can provide onsite support to private sector industrial control system owners and operators, including analytic support (malware, hard drive, and log file analysis) and detailed remediation recommendations.

Over the last few years, the ICS-CERT and the FBI have responded to sophisticated cyber exploitation campaigns against U.S. critical infrastructure industrial control systems (ICS). These campaigns involved two different sets of malware; both of which use tactics to target and gain access to the control systems environments. The characteristics of this activity include the use of ICS zero-day vulnerabilities, malicious ICS payloads, and specific targeting of the operations environment across a variety of sectors including energy, water, critical manufacturing, communications, and more.

ICS-CERT continuously responds to this activity, conducting incident response and analysis, issuing alerts and warnings, and conducting briefings and outreach to highlight these campaigns. ICS-CERT is highly concerned as the sophistication of the threat actors and exploitation techniques used represent an elevated level of risk for critical infrastructure asset owners and operators.

By virtue of the fact that the majority of the nation's critical infrastructure is owned and operated by the private sector, DHS builds and maintains strong partnerships with owners and operators,

recognizing that disruptions and attacks on infrastructure impact homeland security, community resilience, and our economy. This collaboration extends back for many years, with the recent focus on raising awareness of Black Energy and other types of ICS malware. This ICS campaign also included efforts to mitigate the threat and ensure the nation's electric grid protection.

Recent cyberattacks against the power grid in the Ukraine also underscore the importance of maintaining partnerships for risk management in advance of incidents, and applying the full spectrum of capabilities and tools for managing such complex risks.

Conclusion

The electric grid transcends political and geographic boundaries and its operations shift based on demand or availability of natural resources. Innovation has the potential to strengthen some aspects of the grid while at the same time creating new vulnerabilities. Making the grid secure and resilient requires focus on both the grid of today as well as the electric grid of the future. With these realities in mind, the United States and Canada have agreed to develop a joint strategy for strengthening the security and resilience of the North American electricity grid. This strategy will outline a collaborative effort to secure the grid and make it resilient against all hazards, including cyber threats.

The energy industry takes a holistic approach to assessing and mitigating risks from cyber attacks, physical sabotage, and natural disasters, all of which can all result in disruptions to the electric grid. As our nation continues to face increasing and evolving cyber threats and other risks to the U.S. electric grid, the Department must likewise use an integrated approach in preparing for these threats.

In a major step toward this unified approach, the Department proposed to transition NPPD to an operational component, the Cyber and Infrastructure Protection Agency. This transition would elevate cyber operations and provide more comprehensive, coordinated risk management support to our stakeholders that reflect the growing convergence of cyber and physical threats. As one of the current priorities of the Secretary, the Department submitted a plan to the authorizers and appropriators calling for Congressional support and action. The transition, if implemented, would improve the services provided to NPPD's stakeholders. Not only will the transition provide a more comprehensive approach to national level stakeholder engagement and relationship management, but stakeholders in the field will also have access to a unified catalog of services and tools that spans across all of NPPD. For example, the plan proposes to establish regional offices to better integrate field staff like Protective Security Advisors and Cyber Advisors, and support coordinated engagement with electric and other industry partners on cyber and physical vulnerability assessments, information sharing, incident response and other efforts.

We need to position ourselves to successfully address the realities of today's cyber environment and its impacts on critical infrastructure. The proposed structural changes at the headquarters and regional levels will enable NPPD to be more efficient and effectively deliver the important tools

and resources to electric industry partners and other critical infrastructure stakeholders that need them the most. As outlined in my testimony today, the partnership and coordination structures that NPPD facilitates are crucial for supporting both steady-state risk management and incident response. NPPD is committed to ensuring that our partners understand how disruptions and attacks on infrastructure can impact homeland security, community resilience, and our economy, and have the tools to drive informed action to mitigate those risks.

Chairman Barletta, and members of this subcommittee, thank you again for the opportunity to appear before you today to discuss NPPD's efforts in managing the physical consequences of cyber threats.

I look forward to your questions.