Comments on
Draft Outline for the Proposed Joint U.S.-Canadian Electric Grid Strategy

Foundation for
Resilient Societies

August 10, 2016

Foundation for Resilient Societies
52 Technology Way
Nashua NH 03060
603-321-1090

www.resilientsocieties.org

Table of Contents

Introduction

The Foundation for Resilient Societies ("Resilient Societies") appreciates the opportunity to comment on the U.S. Department of Energy ("DOE") Draft Outline for the Proposed Joint U.S.-Canadian Electric Grid Strategy ("Draft Joint Strategy Outline"). Because American and Canadian societies depend on reliable and secure electric power, and because their electric grids are operationally integrated, developing a joint electric grid strategy is vitally necessary to protect the national security, economies, and human population of both countries.

Resilient Societies is a non-profit organization dedicated to the protection of critical infrastructure, including the electric grid. The directors and staff of the Resilient Societies include some of North America's foremost experts on critical infrastructure protection. Through the public docket process and other means, we provide policy recommendations to federal agencies within the United States, including the principal regulator of the U.S. bulk power system, the Federal Energy Regulatory Commission (FERC) and related regulators of critical infrastructure such as the Nuclear Regulatory Commission (NRC).

Resilient Societies regularly participates in standard-setting for electric reliability at the North American Electric Reliability Corporation (NERC), an industry self-regulatory body that sets electric grid reliability standards for both the United States and Canada. We have expended thousands of hours of professional staff time participating in the NERC standard-setting process, including attending in-person meetings of key committees and directly interacting with senior NERC officials. For some important standard-settings at NERC, we have been the only public interest group participating. As a result, our group has gained significant insight into the security and vulnerabilities of the North American electric grid and other critical infrastructures.

The directors and staff of Resilient Societies have been called to testify on electric grid security issues before the U.S. Congress, the Federal Energy Regulatory Commission (FERC), the Canadian Parliament, and multiple U.S. state legislatures. Our recent testimonies to FERC and the Canadian Senate National Security and Defence Committee concerning strategies for electric grid security are appended to this comment in full.

For more information about Resilient Societies, please see our website at www.resilientssocieties.org.

Responses to Specific Queries

The U.S. Department of Energy requested suggestions for improvement of the Draft Joint Strategy Outline. Our responses to specific queries are outlined below.

Risks to Electric Grid Systems

DOE asked for "Suggestions for how best to describe the cyber and physical risks to electric grid systems, as well as ways to address and mitigate those risks." Cyber and physical threats are a subset of major risks to electric grid systems; other major risks include space weather [also termed "solar storms" or "geomagnetic disturbance" (GMD)], nuclear electromagnetic pulse (EMP), intentional electromagnetic interference (IEMI) (also termed "radio frequency weapons") and wide-area natural disasters.

It is notable that the U.S. Government released its National Space Weather Strategy and Action Plan in October 2015 but none of the hazards in this strategy are specifically addressed in the Draft Outline for the Proposed U.S.-Canadian Electric Grid Joint Strategy. A moderate solar storm has already caused a province-wide blackout for Quebec in March of 1989. The omission of space weather and associated solar storms as specific hazards is an obvious deficiency in the Draft Joint Strategy Outline that should be corrected.

The Draft Joint Strategy Outline also omits electromagnetic pulse as a threat to electric grids. In 2008, the U.S. Congressionally-authorized Electromagnetic Pulse Commission determined that "EMP is one of a small number of threats that can hold our society at risk of catastrophic consequences...It has the capability to produce significant damage to critical infrastructures and thus to the very fabric of US society, as well as to the ability of the United States and Western nations to project influence and military power."

At a Technical Conference on June 1, 2016, the U.S. Department of Energy indicated it would develop a strategy and action plan for electromagnetic pulse hazards; and on July 18, 2016 DOE published a joint DOE-Electric Power Research Institute (DOE-EPRI) "Joint Electromagnetic Pulse Resilience Strategy."

Level of Strategic Goals and Objectives

DOE asked for "Suggestions for ensuring that the outlined strategic goals and objectives are at the appropriate level for a joint U.S.-Canadian strategy." We commend the governments of the United States and Canada for initiating a joint electric grid strategy. However:

- The outline as proposed omits significant threats and hazards and therefore could devolve into a document that provides false assurance of safety to the public instead of real action.
- The Draft Joint Strategy Outline does not include an analytic framework to prioritize threats and hazards; a framework that enables prioritized resiliency initiatives is needed.
- Cost-benefit analysis is not proposed as a tool to evaluate and prioritize improvements to grid reliability and security.
- The Draft Joint Strategy Outline lacks any placeholders for specific action steps—for example, better operational planning, installation of protective equipment, or build-out of emergency generation and transmission capacity.
- Were a revised strategy outline to include an "all threats/all hazards" framework to assess investments in resiliency, a resulting Action Plan would be more likely to identify common protection and mitigation measures that are more cost-effective than separate programs for different threats and hazards.
- There is inadequate discussion of the means of implementing potential action steps—for example, voluntary actions by electric utilities or, alternatively, mandatory actions enforced by regulatory standards. The single point vulnerability (SPV) locations are often the same for multiple threats/hazards. There are appreciable cost savings from an all-threats/all-hazards approach since duplication of effort is avoided.

- The Draft Joint Strategy Outline lacks a means to address who will pay for action steps—for example, a program of public and private cost sharing to both improve system reliability and to assure cost-effective recovery from widespread blackouts.

While we recognize that the Draft Joint Strategy Outline may be intended as a general statement of joint intent, remedy of these top-level deficiencies could strengthen this policy document.

Potential Security and Resilience Actions

DOE asked for "Suggestions for actions under the proposed joint strategy that Federal departments and agencies should take to make the grid more secure and resilient." The Draft Joint Strategy Outline lacks any recitation of potential protective actions. Were major grid risks to be appropriately cataloged, policy-makers could evaluate and prioritize a range of protective actions. We show illustrative examples of major grid risks and potential action steps for security and resilience below.

Physical Attack

- Regulatory standards for mandatory protection of control rooms for the sixteen regional Reliability Coordinators. These standards might preclude location in shared office buildings. Standards might require defensible perimeters, armed guards, and force-on-force exercises for these critical facilities.[1]
- Regulatory standards for mandatory protection of large generation plants over 2 gigawatts, totaling approximately 60 locations for the United States and Canada. These standards might require surveillance systems, gunfire locators, armed guards, and force-on-force exercises.[2]

[1]Current reliability standards of NERC for the North American grid have no provisions for physical security of Reliability Coordinators. Under the NERC systems of standards, Reliability Coordinators have sole responsibility for coordination of system restoration after wide-area blackouts.
[2]Current reliability standards of NERC for the North American grid have no provisions for physical security of electric generation plants of any capacity.

Cyber Attack

- Required encryption of communications between electric grid control rooms and transmission substations
- Physical separation of electric grid control systems and the public internet ("air gapping")
- Operational use or backup availability of analog control systems instead of digital control systems
- Supply chain "whitelist" certifications to prevent insertion of malware during the manufacturing process or during firmware updates for critical grid equipment
- Use of "data diodes" to establish one-way communications for certain grid components
- Two-factor authentication for remote access to unattended grid facilities such as transmission substations

Space Weather

- Installation of "neutral ground blocking devices" at transmission substations with Extra High Voltage (EHV) transformers
- Installation of monitors and real-time reporting of Geomagnetically Induced Current (GIC)
- Installation of additional reactive power resources such as Static VAR Compensators (SVC) and synchronous condensers
- Installation of grid monitoring devices (e.g. magnetometers and GIC meters) for warning and improved modeling of GMD coupling to the grid

Nuclear Electromagnetic Pulse Attack

- Installation of "neutral ground blocking devices" and/or ultrafast disconnection relays at transmission substations with Extra High Voltage (EHV) transformers
- Electromagnetic shielding and penetration protection of critical control rooms, such as the control rooms for the sixteen regional Reliability Coordinators in North America
- Stocking of spare components at transmission substations, such as spare circuit breakers and relays

- Ballistic missile defenses and cooperative space launch monitoring programs to prevent high-altitude nuclear detonations whether by missile or by space satellite delivery

Intentional Electromagnetic Interference

- Establishment of perimeters around critical control rooms with sufficient distance to attenuate electromagnetic interference
- Shielding of critical grid facilities and/or component equipment
- Stocking of spares for components susceptible to permanent damage from electromagnetic interference
- Installation of IEMI warning sensors at control sites

Wide-Area Natural Disasters

- Operational plans to "island" electric grid networks and to identify grid boundaries where disconnects are feasible
- Plans for large-scale deployment of federal government and electric utility resources for grid restoration
- Standards for renewable generation and transmission systems, including hydroelectric plants, that might be used for blackstart recovery of the bulk electric system
- Exercises to practice restoration and recovery from major outages

New Ways to Secure the Future Electric Grid

DOE asked for "Suggestions for new ways to secure the future grid across North America, as outlined in the final section." The longstanding lack of government strategies and mandatory standards to secure the electric grid has forestalled commercial development of technical solutions. In some cases, when private capital has been invested, stonewalling by electric utilities has threatened to make innovative products economically unviable. For example, a private businessman has invested millions of dollars developing and testing a "neutral ground blocking device" to protect electric grid systems against both space weather and nuclear electromagnetic pulse attack. Electric utilities have opposed mandatory standards for hardware-based protection; as a result, only one blocking device has been installed in the entire

North American electric grid. Articulated government strategies and action plans are essential steps to motivate private industry to develop new ways to secure the current and future electric grid.

Timelines for Planning and Investment

DOE asked for "Suggestions for timelines to use when considering future planning and investment opportunities." When commercial solutions are available and cost-effective, the timeline for planning and investment could be short—five years or less. For example, full deployment of neutral ground blocking devices to protect against space weather could be accomplished by 2020.[3] For grid threats requiring new research and development, or where costs might be substantial, a timeline of 25 years may be necessary. For example, schemes for protection of electric generation plants against nuclear electromagnetic pulse are still to be developed.

Comments on Proposed Outline for Grid Strategy

The proposed Draft Joint Strategy Outline is a good first step. However, the outline as proposed has significant gaps and shortfalls. Below we recite the major headings and subsections of the proposed outline, inserting our comments and suggesting additional headings. The original Draft Joint Strategy Outline is reproduced below in non-bolded black font. Our comments are in bold black font; our suggested additional headings are in bold red font.

Introduction and Context for the Joint U.S.-Canadian Electric Grid Strategies

The introductory and context-setting sections of the joint strategy will describe the context for the joint strategy. **Comment: The context for the joint strategy should be the existential threat to the United States and Canada of an unsecured electric grid. Wide-area and**

[3] Some components of protective equipment in neutral blockers for solar storms will require EMP hardening against ultrafast E1 pulses if that equipment is intended to protect against both solar storms and man-made EMP. See e.g. Vladimir Gurevich, "Impacts of Magnetohydrodynamic Effect of HEMP on Power Equipment: Problems and Solutions," *Int'l J. Applied Sci. Engr*. (2016) 14: 49-58, esp. pp. 55-56. The specific sub-components cited by Dr. Gurevich as vulnerable to E1 pulses are, according to Emprimus, already hardened to protect against E1 pulses. Independent third-party testing of protective equipment should be a component of any grid protection strategy.

long-term loss of electric power could result in loss of the majority of the American and Canadian populations.

Goal 1: Protect Today's Grid and Enhance Preparedness

This section will outline opportunities to avoid, deter, and mitigate risks before they impact the grid. This includes information sharing between and among owners, operators, public, private and third-party participants whose protection of critical assets would benefit from actionable threat and hazard information and would provide information utilization for prudent and efficient security investments. This section will also highlight the importance of coordinating ongoing law enforcement, emergency management, reliability coordination, and monitoring and detection activities, the practice of which will improve protection capabilities. **Comment: We find it notable that "information sharing" and "coordination" have taken preeminent roles in the Draft Joint Strategy Outline, as evidenced by their recitation upfront in Goal 1. Too often these steps have been promoted by electric utilities as substitutes for the most important goal of tangible protective actions—such as installation of hardware-based protection. We suggest that "information sharing" and "coordination" take less prominent roles in the Draft Joint Strategy Outline.**

This section will also address the method of preparedness that identifies can't-lose aspects of the system to mitigate the outer limit of tolerable impacts to the grid. This section will address major isolated as well as potentially cascading events that create out-and-out system failure or balloon into major regional or multi-system impacts. This section will examine how to create necessary incentives and investments to engage the protective measures for outlier events. The section will close by examining the electric grid's interdependencies with other critical systems and functions of the nations' economies and societies. Given our economic and social reliance on electricity, the strategy will identify the importance of securing the grid in the broader context of our joint and domestic national security goals. **Comment: The topics proposed for this section are generally a good start. However, the Draft Joint Strategy Outline is currently light on specifics. For example, the "cascading events that risk complete system failure" should be specifically listed.**

Objective 1. Enhance Information Sharing

i. Enhance information sharing between government and industry. **Comment: Listing "enhance information sharing" as the very first element of Objective 1 creates the impression that this would be one of the most important elements of a grid protection strategy.**

ii. Build organizational capacity to improve government, and industry information sharing and support to improve management of risk critical to the success of business mission and goals. **Comment: Statements such as "improve management of risk critical to the success of business**

mission and goals" are jargon that provides no meaningful guidance. "Information sharing" should have a less prominent role in the Draft Joint Strategy Outline.

Objective 2. Develop and Coordinate Existing Forensic and Law Enforcement Capabilities

i. Improve tools, processes, and coordination among relevant government entities and industries for monitoring, detecting, analyzing, reporting, defending and mitigating threats to the electric grid. **Comment: Increased forensic and law enforcement capabilities would be more effective if targeted to specific grid threats.**

Objective 3. Deter Major Isolated and Cascading Events

i. Protect critical assets from relevant adversarial, natural, and technological threats to prevent and mitigate power loss and system failure. **Comment: Relevant grid risks should be specifically enumerated. "Hazards," which are caused by naturally-occurring events, should be separated from "threats," which are caused by human intent. The process of enumerating threats and hazards could also be used as a means to prioritize risks. For example:**

1. **Physical attack**
2. **Cyber-attack**
3. **Space weather**
4. **Nuclear electromagnetic pulse**
5. **Intentional electromagnetic interference**
6. **Wide-area natural disasters**

ii. Develop guiding principles for automatic and manual means of preventing cascading blackouts (System Operations). **Comment: If automated reporting of electric grid flows and operational status to governments is to be a part of the Draft Joint Strategy Outline, this would be a good place to insert it.**

Objective 4. Align Standards, Incentives and Investment with Security Goals

i. Align utility incentives for planning and investment with regulatory processes and tools for prudent cost recovery, including tools for security valuation. **Comment: We suggest the alternative wording, "Align utility incentives for investment in prioritized security improvements combined with regulatory actions that would allow cost recovery cost-sharing among utility owners, electric rate-payers, and taxpayers."**

Objective 5. Understand and Mitigate Vulnerabilities From Interdependencies With Other Critical Infrastructures

i. Mitigate and reduce security risks/vulnerabilities caused by interdependence between grid technologies and other infrastructures, including telecom, water, and natural gas. **Comment: Because railroads transport coal for power plants that generate approximately one-third of U.S. electricity, we suggest adding "rail transport" to the specific list of**

interdependent infrastructures. Since grid control depends in large part on the public internet, we suggest that this be added to the critical infrastructure list.

ii. Identify and manage impacts to other critical societal functions (e.g., defense). **Comment: "Other critical societal functions" should be specifically enumerated. For example, national defense, state and local government, law enforcement, and healthcare.**

Goal 2: Manage Contingencies and Enhance Response and Recovery Efforts

This section will address response and recovery options during and after an incident, examining public and private resources available, including through mutual assistance efforts for physical and cyber capabilities. This section will also highlight the complexity and potential issues with supply chains, which are compounded in an emergency. Finally, this section will highlight the importance of adaptation through recovery and rebuilding efforts, restoring capabilities through smarter, more efficient, and forward-looking solutions. **Comment: "Restoring capabilities through smarter, more efficient, and forward-looking solutions" is jargon that sounds good but means very little unless "solutions" or potential action steps are enumerated and prioritized. The goal description should include cooperative table-top and field exercises of contingency response plans.**

Objective 1. Improve Emergency Response and Continuity

i. Enhance public and private resources for response to and recovery from major loss-of-power events. **Comment: The use of the terms "public and private resources" is too general. What resources of the federal government, state governments, local governments, or all three are applicable? Federal power authorities have freedom to adopt higher reliability standards than mandated by NERC-FERC standards. How could federal power authorities provide leadership through demonstration programs? What can Canadian Provinces do to advance grid reliability? Would "private resources" come from electric utilities, non-governmental organizations, or private citizens? More specific identification of "resources" would inform the grid strategy.**

Objective 2. Develop or Enhance Mutual Assistance for Physical, Cyber, and Electromagnetic Threats and Space Weather Hazards

Comment: Objective 2 should also specifically include electromagnetic threats and natural hazards, i.e. "Mutual Assistance for Physical, Cyber, and Electromagnetic Threats and Space Weather Hazards."

i. Foster robust mutual assistance programs for physical grid assets, and develop a cybersecurity mutual assistance program. **Comment: Mutual assistance should not be limited to "physical grid assets" and "cybersecurity." For example, mutual assistance could extend to emergency fuel supply and transport, control room operations, and contingency generation and transmission after other events. We note that "mutual assistance" is a specific action step; placeholders for other action steps should be appropriate in the Draft Joint Strategy Outline. Moreover, because Canadian energy projections anticipate increased export of hydroelectric, wind and other renewable energy from Canada to the United States[4], what**

[4] The National Energy Board *Canada's Energy Future 2016 Report, Energy Supply and Demand Projections to 2040*, Ottawa, January 2016, Chapter 8, "Electricity Outlook," projects modest increases in exports of electricity, mainly

joint policies will assure resiliency, including reliable cranking paths for blackstart of the entire North American electric grid?

Objective 3. Identify Dependencies and Supply Chain Needs During an Emergency

i. Address effects from power outages, such as loss of services. **Comment: Increasingly, federal agencies and the U.S. Congress through legislation are recognizing supply chain risks for large power transformers. The Draft Joint Strategy Outline should specifically identify large power transformers as a critical supply chain issue.**

Objective 4. Recover and Rebuild

i. Adapt via recovery to result in more resilient investments, practices and processes. **Comment: Few in government or industry would object to "more resilient investments, practices and processes," but what would this mean in practice? More specific action steps in the Draft Joint Strategy Outline are appropriate.**

Objective 5 Manage Environmental Consequences of Long-Term Grid Outages

Comment: Long-term grid outage would have severe environmental consequences. Without electric power for control, chemical plants and other industrial facilities could release large quantities of toxins. Wastewater treatment systems would cease functioning. Deprived of electricity for cooling, nuclear power plants and their spent fuel pools could release clouds of radioactive material. The Draft Joint Strategy Outline needs specific consideration of environmental consequences and proposed action steps to avert and to mitigate these consequences.

Goal 3: Build a More Secure and Resilient Future Grid

The final section of the strategy will take on the challenge and opportunities to adapting through recovery efforts, underscoring the end-goal of grid resilience. The first part of the final section will explore post-incident actions in the context of evolving grid design, technologies, and a changing climate (that is, the potential impact of more frequent and severe natural disasters). The first part of this section will also address the opportunities to develop and advance the deployment of tools and technologies to address the security vulnerabilities addressed in this strategy.

The second part of this final section will outline opportunities to integrate security and resilience into planning, investment, regulatory- and policy-decision making for joint, cross-border security goals. This includes enhancing modeling and risk analysis capabilities to characterize vulnerabilities for decision-making and investments, suggesting ways to align utility and market incentives, and addressing workforce risks and opportunities for evolving technical knowledge needs. Finally, this section will point to the importance of pursuing optimal domestic security goals to coordinate cross-border where possible, and noting where domestic-specific goals do not lend themselves to joint coordination.

---

hydroelectric, solar and wind generation-based, to the United States. See in particular Figure 8.5, "Net Exports of Electricity and Interprovincial Transfers, Reference Case," at p. 85. In the event of accelerated U.S. retirements of fossil fuel generation under the EPA Clean Power Plan, Canadian electrical exports could exceed those of the *Energy Futures 2016* projected Reference Case through year 2040.

Objective 1. Understand and Manage New and Evolving Risks From Grid Technologies and Grid Design

i. Identify, understand, and, to the extent possible, neutralize emerging threats (including through supply chains). **Comment: Ill-considered grid technologies and grid design are causing "emerging threats." Below are some examples. The Draft Joint Strategy Outline would benefit from including specific categories of "emerging threats" and naturally-occurring hazards.**

Physical Security

- **Critical facilities that inherently lack any capability for a defensive perimeter, both in normal operation and during emergencies**
- **Backup facilities with the same physical or cybersecurity vulnerabilities as the primary location**
- **Co-siting of very large generation plants in close physical proximity**
- **Installation of physical security electronic systems with cyber and intentional electromagnetic effects (IEMI) vulnerabilities**

Cybersecurity

- **Supply chain vulnerabilities due to use of equipment with hard-coded passwords, cybersecurity "back doors," or other built-in vulnerabilities**
- **Remote access to substation and generation equipment by equipment vendors in order to minimize operational and maintenance costs; several of these vendors have large market share and therefore cybersecurity breaches could affect many facilities**
- **Increased reliance upon unmanned transmission substations that cannot quickly switch to manual operations in event of cyberattack or telecommunications loss**
- **Removal of manual control capability when digital controls are installed in legacy facilities such as hydroelectric plants**
- **Dependence on Global Positioning System (GPS) timing resources that rely on satellites and ground stations vulnerable to solar storms, nuclear electromagnetic pulse, jamming, or cyber-spoofing**

Long Distance Electricity Transmission

- **Bulk transmission of electricity over long distances to minimize rates or provide competition in capacity auctions**
- **Bulk transmission of electricity over long distances to comply with environmental regulations**
- **System instability when a small number of critical bulk transmission substations are attacked or otherwise lost**
- **Increased electric transmission system vulnerability to solar geomagnetic or man-made electromagnetic pulses because of higher voltages, lower line resistance, and longer average line lengths**

Fuel Security

- **Accelerating closure of U.S. coal-fired generation plants that typically have 50-100 days of bituminous and subbituminous coal on site and their replacement with gas-fired plants dependent on just-in-time fuel delivery through long pipelines**

- **Mismatches of interstate gas pipeline capacity supply, demand, and direction of flow, combined with high variability of gas produced by hydraulic fracturing; variability is due to price fluctuations and rapid well depletions**
- **Closure of nuclear plants with 1-2 years of latent fuel stored in reactor cores; closures are due to inability to compete in competitive auctions for electricity capacity that consider price but not fuel security**
- **Closure or redesign of "dual fuel" generation plants and replacement with plants relying on a single fuel source such as natural gas**
- **Interdependence with interstate natural gas pipelines having electrically-actuated gas compressors and automated control systems dependent on electricity from the commercial grid**
- **Interdependence with interstate natural gas pipelines not having mandatory reliability coordination and not subject to mandatory reliability and cybersecurity standards**
- **Conflicts between capacity planning windows for electricity generation and natural gas transmission**
- **Capacity constraints of natural gas pipelines used for electricity generation combined with the predominant reliance on (cheaper) non-firm gas contracts that are at risk of supply diversion to heating customers during polar vortex events**
- **Lack of fuel diversity within large geographic regions and corresponding overreliance on natural gas**

Essential Reliability Services

- **Declining or inadequate generation reserve margins**
- **Loss of voltage control, frequency support, and reactive power formerly provided by mechanical inertia and other characteristics of generators in fossil fuel and nuclear plants**
- **Increasing reliance on non-dispatchable power sources such as wind and solar**
- **Increasing reliance on internet and digital control systems vulnerable to cyber attacks**
- **Closure or minimization of blackstart resources to comply with cybersecurity standards or environmental regulations**[5]

Contingency Planning

[5] Blackstart assets, traditionally hydroelectric and coal generating plants, are increasingly reliant on natural gas generating facilities. In its *Canada's Energy Future 2016 Report*, the National Energy Board of Canada projects a modest increase in net exports of electricity to the United States through year 2040. See Canada's Energy Future 2016: Energy Supply and Demand Projections to 2040, Jan. 2016, ch.8, Fig. 8.5, "Net Exports of Electricity and Interprovincial Transfers, Reference Case," p.85. In the event of rapid transition from fossil fuels to renewables in the United States, per the Clean Power Plan proposed by the U.S. Environmental Protection Agency, NEB projects a still higher dependency on Canadian power exports to the United States. Reliability risks may be exacerbated, especially in the New York ISO and ISO New England regions, where underground gas storage capacity is constrained, and which together receive about 60 percent of the total of Canadian electricity exported to the U.S. annually. Loss of nuclear baseload, diversion of interstate gas supplies to firm heating customers during polar vortexes, vulnerability of long distance electric transmission, risks of solar storm damage to grid equipment and other risks need combined assessment to identify best practices for improving electric reliability in the Northeastern regions of the U.S. and Canada.

- **The practice of building multiple transmission lines close to a single path and not including loss of all transmission lines along that single path in N-1 and N-2 planning criteria**
- **The practice of routing multiple transmission lines through a single substation and not including loss of all transformers in the single substation in N-1 and N-2 planning criteria**
- **The practice of building multiple generation plants largely or totally dependent on a single natural gas pipeline and not including loss of this single pipeline in N-1 and N-2 planning criteria**
- **Not including a scenario for loss of all generation units at a single site in N-1 and N-2 contingency planning, or not including simultaneous loss of multiple generation facilities that are essentially at the same physical location, including situations where generation facilities are separately owned and/or operated but in close proximity**
- **N-1 and N-2 contingency planning that assumes Reliability Coordinators can depend on resources in neighboring control areas, even when an initiating event may affect multiple control areas simultaneously—cyberattacks and solar geomagnetic storms being prime examples**
- **System restoration drills that assume cascading outages but do not take into account scenarios for equipment damage**

Communications Security

- **Electric grid operation and restoration planning that depends on commercial telecommunications systems with typically 1-3 days of diesel fuel for backup generators**
- **Use of the public internet to communicate operational data for the electric grid**
- **Use of cell phone networks to communicate with grid substations and for other operational data flows when these networks are vulnerable to radio jamming and Global Positioning System (GPS) signal loss**
- **Dependence on communications systems not designed to withstand geomagnetically induced currents or nuclear electromagnetic pulse**

Other Emerging Threats

- **Compliance with environmental regulations that do not take into account needed resilience to protect against concurrent fuel losses, generation outages, increased reactive power demand, or extended loss of alternating current (AC) power during low frequency events**[6]
- **Lack of protection for reactor vessels and spent fuel pools at nuclear plants against Extended Loss of Offsite AC Power (ELAP).**
- **Widespread use of custom designs for large power transformers, negating benefits of shared reserve transformer fleets**
- **Displacement of hydroelectric and coal-fired plants by natural gas-fired generation for blackstarting the grid**

ii. Ensure that continued integration of grid and IT infrastructures accounts for the security benefits and challenges of that enhanced integration. **Comment: Use of the public internet for electric grid communications, including communications for the so-called "smart grid," vastly**

[6] The Canadian Electricity Association report, Adapting to Climate Change, Jan. 2014, at page 4, observes: "While increased demand from the United States and changes in water availability may present opportunities, climate change presents considerable risks to service reliability."

increases the cyber-attack surface. The Draft Joint Strategy Outline needs to specifically address vulnerability and risks from connection of the public internet to electric grid systems.[7]

iii. Meet national security goals in a changing climate and energy landscape. **Comment: The Draft Joint Strategy Outline could benefit from a more specific recitation of "national security goals," as well as a more specific description of factors in the "changing climate and energy landscape."**

iv. Improve preparedness in the context of increased natural disaster intensity and frequency and integrate security considerations into energy policy making, as well as utility and project planning, design, and implementation. **Comment: Most natural disasters such as floods, tornadoes, and ice storms are localized events and therefore would not cause wide-area and long-term grid outage. With the exception of major hurricanes (such as SANDY in year 2012) or tsunamis (which precipitated the Fukushima Dai-ichi nuclear disaster in year 2011), most natural disasters should receive lower priority in the Draft Joint Strategy Outline. We note that "natural disasters" are not consistently included as hazards in the Draft Joint Strategy Outline; instead, "cyber and physical risks to electric grid systems" seem to be the two major specified risks. A key element of joint strategy, to be supported by adequate discussion and analysis, should be devoted to the avoidance of widespread, long-term outages due to scenario-events that have not yet occurred—especially events that could cause nearly simultaneous continental-scale effects, *viz.*, GMD and EMP.**

Objective 2. Develop and Deploy Security and Resilience Tools and Technologies

i. Ensure that the technological and institutional and architectural evolution of the grid enhances security and resilience. **Comment: The current lack of national strategies for grid security is causing the grid to evolve into architectures and technologies that increase cumulative risks. A prime example is overdependence on power transmission lines that run for hundreds of miles and are not protected against hazards such as space weather. For example, the State of California imports approximately 30% of its electric power over long-distance transmission lines. For example, the New England states import approximately 10% of their power over long-distance transmission lines from Quebec; these lines have already tripped off during small solar storms.**

ii. Be resilient to, and secure against, a range of grid threats. **Comment: More detail for the "range of grid threats" would inform policy-makers.**

iii. Coordinate with industry and operator practices to detect and mitigate grid anomalies quickly and effectively. **Comment: More detail in the specification of "grid anomalies" would inform policy-makers.**

[7] It is notable that on July 21, 2016 the Federal Energy Regulatory Commission initiated a Notice of Inquiry to address risks of internet access to control centers and control equipment within the U.S. bulk electric system.

Objective 3. Integrate Security and Resilience Into Planning, Investment, Regulatory- and Policy-Decision Making, and Coordinate Cross-Border Grid Integration Between the United States and Canada

i. Enhance modeling and risk analysis capabilities to better characterize grid vulnerabilities, understand impacts of loss-of-power events, and support risk-informed decisions, including investments. **Comment: Costs and benefits of protective actions should be quantitatively modelled, in addition to modelling of risks.**

ii. Align utility and market participant incentives for planning and investment with regulatory processes and tools for prudent cost recovery, including tools for security valuation. **Comment: It is not clear whether "tools for security valuation" refers to the valuation of debt and equity in investor-owned utilities or the valuation of security improvements to the electric grid. Better phrasing might be "tools for valuing grid security improvements."**

iii. Continue to pursue optimal domestic planning, investment, regulatory- and policy-decision making for security and resilience, noting where domestic-specific approach do not lend themselves to joint coordination. **Comment: Rarely is government planning or decision-making "optimal." Alternative wording might be "Continue to pursue planning, investment, regulatory- and policy-decision making for security and resilience that meets country-specific goals and priorities, noting where a country-specific approach does not lend itself to joint coordination."**

iv. Address the need to reinforce existing and develop new workforce capabilities. **Comment: If this subsection refers to the shortage of skilled labor for electric grid maintenance and operations, it should specifically state this. Or if the subsection is meant to say that additional workforce capability for cybersecurity will be required, it should specifically state this.**

v. Formalize a joint U.S.-Canada process for policy-making and planning for electric grid security. Comment: Currently there is no obvious forum for the *governments* of the United States and Canada to jointly plan improvements to electric grid security. NERC coordinates among utility entities in North America, but industry-only coordination has delayed hardware protections against solar storms and man-made EMP, cyber-protection for industrial control systems within the bulk power system, and cyber-protection of industrial control systems at interdependent infrastructures such as natural gas transmission and storage. In the United States, regulatory responsibility is divided among the Department of Energy, the Federal Energy Regulatory Commission, the Nuclear Regulatory Commission, the Department of Transportation, and public utility commissions of the fifty states. In Canada, regulation of electric grid security is at the provincial level.

Conclusion

We appreciate that the governments of the United States and Canada have initiated a process to jointly agree on a strategy for electric grid security. However, the Draft Joint Strategy Outline suffers from obvious deficiencies—most notably, the outline does not enumerate specific electric grid threats and hazards that have been identified by government bodies, including the hazard of space weather and the threat of electromagnetic pulse. The outline does not propose a mechanism for prioritizing grid risks. Environmental consequences of long-term grid outages are not addressed. Potential action steps are not described in sufficient detail to inform policy-makers and the public. We hope that these deficiencies will be remedied in future versions of the Draft Joint Strategy Outline.

Given the importance of electric grid security, it may be appropriate for DOE to hold a public hearing on the Draft Joint Strategy Outline and accept testimony from interested parties.

Appendix 1—Testimony of Resilient Societies to FERC

UNITED STATES OF AMERICA

BEFORE THE

FEDERAL ENERGY REGULATORY COMMISSION

Reliability Technical Conference **Docket No. AD16-15-000**

TESTIMONY OF THE FOUNDATION FOR RESILIENT SOCIETIES

By Thomas S. Popik, Chairman
At the June 1, 2016 Reliability Technical Conference
Submitted to FERC on May 6, 2016

My name is Thomas Popik, and I am chairman of the Foundation for Resilient Societies, a non-profit group dedicated to the protection of critical infrastructure, including the North American electric grid. Since 2011, Resilient Societies has frequently participated in standard-setting at the North American Electric Reliability Corporation (NERC) and rulemaking before the Federal Energy Regulatory Commission (FERC). Our group includes well-known experts in critical infrastructure protection. We appreciate that the FERC Commissioners gave us this opportunity today to provide testimony on grid security that diverges markedly from electric utility industry viewpoints.

For several years running we have heard from NERC that the Bulk Power System has achieved an "Adequate Level of Reliability." This optimistic assessment relies on past operating statistics. However, a whole class of grid security threats—so-called *High Impact, Low Frequency events*—have not yet occurred during the sampling periods examined by NERC; therefore, performance against these threats falls outside of positive NERC metrics. For more information, see our filing on Docket No. AD16-15-000 containing the work of Charles Mo, a professional statistician retained by Resilient Societies.

According to Resilient Societies' own risk assessments, four threats have potential to take down electric grids and other interdependent infrastructures over large regions for months or years, causing catastrophic military, economic, societal, and environmental impacts: physical attack, cyberattack, electromagnetic pulse, and solar storms. All of these *High Impact, Low Frequency events* have the potential for impact over continental scales such that that no significant mutual assistance would be reliably available, and even international assistance could be significantly delayed. The duration of resulting blackouts could last weeks, months, or years.

A number of factors continue to heighten grid vulnerability to *High Impact, Low Frequency events*, including:

Fuel Security

- Accelerating closure of U.S. coal-fired generation plants that typically have 50-100 days of bituminous and subbituminous coal on site[8] and their replacement with gas-fired plants dependent on just-in-time fuel delivery through long pipelines[9]
- Mismatches of interstate gas pipeline capacity supply, demand, and direction of flow, combined with high variability of gas produced by hydraulic fracturing; variability is due to price fluctuations and rapid well depletions[10]
- Closure of nuclear plants with 1-2 years of latent fuel stored in reactor cores; closures are due to inability to compete in competitive auctions for electricity capacity that consider price but not fuel security
- Closure or redesign of "dual fuel" generation plants and replacement with plants relying on a single fuel source such as natural gas
- Interdependence with interstate natural gas pipelines having electrically-actuated gas compressors and automated control systems dependent on electricity from the commercial grid
- Interdependence with interstate natural gas pipelines not having mandatory reliability coordination and not subject to mandatory reliability and cybersecurity standards
- Conflicts between capacity planning windows for electricity generation and natural gas transmission
- Capacity constraints of natural gas pipelines used for electricity generation combined with the predominant reliance on (cheaper) non-firm gas contracts that are at risk of supply diversion to heating customers during polar vortex events
- Lack of fuel diversity within large geographic regions and corresponding overreliance on natural gas

Essential Reliability Services

- Declining or inadequate generation reserve margins
- Loss of voltage control, frequency support, and reactive power formerly provided by mechanical inertia and other characteristics of generators in fossil fuel and nuclear plants
- Increasing reliance on non-dispatchable power sources such as wind and solar
- Closure or minimization of blackstart resources to comply with cybersecurity standards or environmental regulations

---

[8] As of February 2016, the average U.S. "days of burn" for bituminous coal was 99 days; and was 105 days for subbituminous coal at coal-generating electric plants. See U.S. Energy Information Administration (EIA), "Days of burn by non-lignite coal rank, January 2009 – February 2016," released April 28, 2016. Over the past five years, "days of burn" has rarely been less than 50 days. Available at https://www.eia.gov/electricity/monthly/update/fossil_fuel_stocks.cfm#tabs_stocks2-1 .

[9] See EIA, "Scheduled 2015 capacity additions mostly wind and natural gas; retirements mostly coal," released March 10, 2015, available at http://www.eia.gov/todayinenergy/detail.cfm?id=20292#.

[10] See EIA ," Hydraulically fractured wells provide two-thirds of U.S. natural gas production," released May 5, 2016, available at http://www.eia.gov/todayinenergy/detail.cfm?id=26112.

Contingency Planning

- The practice of building multiple transmission lines close to a single path and not including loss of all transmission lines along that single path in N-1 and N-2 planning criteria
- The practice of routing multiple transmission lines through a single substation and not including loss of all transformers in the single substation in N-1 and N-2 planning criteria
- The practice of building multiple generation plants largely or totally dependent on a single natural gas pipeline and not including loss of this single pipeline in N-1 and N-2 planning criteria
- Not including a scenario for loss of all generation units at a single site in N-1 and N-2 contingency planning, or not including simultaneous loss of multiple generation facilities that are essentially at the same physical location, including situations where generation facilities are separately owned and/or operated but in close proximity
- N-1 and N-2 contingency planning that assumes Reliability Coordinators can depend on resources in neighboring control areas, even when an initiating event may affect multiple control areas simultaneously—cyberattacks and solar geomagnetic storms being prime examples
- System restoration drills that assume cascading outage but do not take into account scenarios for equipment damage

Communications Security

- Electric grid operation and restoration planning that depends on commercial telecommunications systems with typically 1-3 days of diesel fuel for backup generators
- Use of the public internet to communicate operational data for the electric grid
- Use of cell phone networks to communicate with grid substations and for other operational data flows when these networks are vulnerable to radio jamming and Global Positioning System (GPS) signal loss
- Dependence on communications systems not designed to withstand geomagnetically induced currents or nuclear electromagnetic pulse

Physical Security

- Critical facilities that inherently lack any capability for a defensive perimeter, both in normal operation and during emergencies
- Backup facilities with the same physical or cybersecurity vulnerabilities as the primary location
- Co-siting of very large generation plants in close physical proximity

Cybersecurity

- Supply chain vulnerabilities due to use of equipment with hard-coded passwords, cybersecurity "back doors," or other built-in vulnerabilities
- Remote access to substation and generation equipment by equipment vendors in order to minimize operational and maintenance costs; several of these vendors have large market share and therefore cybersecurity breaches could affect many facilities
- Increased reliance upon unmanned transmission substations that cannot quickly switch to manual operations in event of cyberattack or telecommunications loss
- Removal of manual control capability when digital controls are installed in legacy facilities such as hydroelectric plants
- Dependence on Global Positioning System (GPS) timing resources that rely on satellites and ground stations vulnerable to solar storms, nuclear electromagnetic pulse, jamming, or cyber-spoofing

Long Distance Electricity Transmission

- Bulk transmission of electricity over long distances to minimize rates or provide competition in capacity auctions
- Bulk transmission of electricity over long distances to comply with environmental regulations
- System instability when a small number of critical bulk transmission substations are attacked or otherwise lost
- Increased electric transmission system vulnerability to solar geomagnetic or man-made electromagnetic pulses because of higher voltages, lower line resistance, and longer average line lengths

Other Factors

- Compliance with environmental regulations that do not take into account needed resilience to protect against concurrent fuel losses, generation outages, increased reactive power demand, or extended loss of alternating current (AC) power during low frequency events[11]
- Lack of protection for reactor vessels and spent fuel pools at nuclear plants against Extended Loss of Offsite AC Power (ELAP).
- Widespread use of custom designs for large power transformers

[11] We note that proposed Sec. 4301 of S. 2012, the Energy Policy Modernization Act of 2016, which passed the U.S. Senate and is awaiting a House-Senate Conference, would mandate "Bulk-power system reliability impact statements" requiring consideration of NERC and FERC comments before final rulemaking by other agencies. Recent U.S. generation plant closures and pending facility closures have not utilized these planning safeguards.

Responses to FERC's Written Questions

New Authorities in Recent Cybersecurity Legislation

Questions: The Cybersecurity Information Sharing Act of 2015 (CISA 2015) and the Fixing America's Surface Transportation (FAST) Act both addressed cybersecurity. Discuss how government, NERC and industry can use these new authorities to address cybersecurity risks and enhance information sharing.

Prepared Response: For cybersecurity defense of the North American electric grid, lack of real-time situational awareness and insufficient command and control for operational response are shortfalls in the current system managed by Reliability Coordinators, Balancing Authorities, Transmission Operators, and Load-Serving Entities. CISA 2015 provides voluntary mechanisms for real-time information collection and dissemination, a major step forward for situational awareness. FAST provides for centralized command and control at the U.S. Department of Energy (DOE) during grid emergencies.

However, for these new legal authorities to be effective, FERC must establish additional reliability standards and operational processes well in advance of any grid emergency. While CISA 2015 establishes liability protection for voluntary information sharing, additional legal authority within Section 215 of the Federal Power Act could mandate real-time cybersecurity information sharing by utilities by means of reliability standards. Likewise, rules promulgated by the Department of Energy under the Administrative Procedure Act could establish processes for operational control of the Bulk Power System either through communication to Reliability Coordinators or by direct electronic means.

Under the current NERC standards for cybersecurity incident reporting, registered entities appear to be gaming the system by finding ways to make incidents non-reportable or intentionally not identifying incidents. For example, in all of 2014 NERC recorded only 3 reportable cybersecurity incidents. While the 2015 State of Reliability Report is not available at the time of this draft, our understanding is that in all of 2015 NERC recorded zero reportable cybersecurity incidents. In contrast, in 2014 the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) of the U.S. Department of Homeland Security received 79 reported cybersecurity incidents from the Energy Sector. In 2015, US-CERT received 46 reported cybersecurity incidents from the Energy Sector. It is improbable that electric utilities are immune from cybersecurity incidents that affect the Energy Sector generally. We also note that Admiral Michael Rogers, Director, National Security Agency and Commander of U.S. Cyber Command, testified to Congress on November 20, 2014 that multiple foreign nations can take down the U.S. grid—this statement is inconsistent with trivial numbers of cybersecurity incidents reported to NERC by electric utilities.

Clearly there is a gap in NERC cybersecurity incident reporting; this gap should be addressed by more stringent FERC-mandated reporting standards. As part of the same standards development process, near-real-time electronic reporting could be established.

Lessons from Recent Attacks on Electric Grids

Questions: What can we learn from recent attacks, and what should we do in response? Are there ways to reduce risk by "simplifying" or even non-digitizing the technology used at certain critical points or locations? Are there reasonable ways to further reduce the risk of lengthy outages from hostile actions, and can new standards or changes to standards help?

Prepared Response: In the set of recent attacks on electric grids, we include the April 2013 rifle attack on the Metcalf Substation; the June 2014 incendiary attack on the Nogales, Arizona generation facility and substation; the December 2014 airborne attack on long-distance transmission lines of Hydro-Quebec; the March 2015 disabling of Supervisory Control And Data Acquisition (SCADA) equipment at the Westpark substation near Bakersfield, California; the November 2015 explosive attack on transmission lines in the Russian-annexed territory of Crimea; and the December 2015 cyberattack on distribution utilities in Ukraine.

The Metcalf attack was operationally sophisticated and well-planned, targeting the principal substation supplying a peninsula containing Silicon Valley and San Francisco. The Nogales attack targeted the end of a radial line serving a large border crossing station. The Hydro-Quebec attack used methods employed by military forces to disable high voltage transmission lines. The targeting of SCADA equipment at Westpark substation raises concerns about selective compromise of control systems. The Crimea attack targeted radial lines serving a peninsula and appears to be an act of war. The Ukraine cyberattack was technically sophisticated and appears to be an act of war.

The fact that the Ukrainian grid did not suffer significant permanent equipment damage is more likely to be the result of the attack sponsor seeking to demonstrate grid take-down capabilities without the intent to cause permanent grid damage. The same sponsor had the capability to rapidly open and close circuits and to cause permanent damage to rotating grid equipment, the so-called AURORA attack that remains a key vulnerability of the U.S. electric grid.[12]

A quick takeaway is that peninsulas—either physical or "electricity peninsulas" served by radial lines—are targets. A more important conclusion is that grid attacks are increasingly on critical facilities, using military techniques that have become standard components of modern "information warfare." In some cases, these attacks may be "test runs" for terrorists or foreign adversaries. We use this conclusion to introduce two important strategic concepts:

1. Critical infrastructure will become a battlefield of the future
2. Military-type defenses for the most critical infrastructure are therefore necessary

[12] Fifteen reforms are proposed for FERC consideration in a Joint Filing in FERC Docket RM15-14-000 and Docket RM15-14-001 (Request for Rehearing of Order No. 822, pending) submitted by the Foundation for Resilient Societies, Isologic LLC, and Applied Control Solutions LLC on March 29, 2016.

Critical Infrastructure Will Be a 21st Century Battlefield

War in the first half of the 20th century was characterized by battles between massed ground and naval forces supported by air power. In the second half of the 20th century, wars were increasingly fought against terrorists and insurgencies in countries far from North America.

When terrorists launch an attack directly against humans, as they did on September 11, 2001, it is an assault against the idea of an open and free society—and a tragedy for the individuals and cities directly affected. Were terrorists or a foreign power to launch an effective infrastructure attack against the United States and its Allies, it could threaten the continued existence of our countries—and result in millions of deaths. Conversely, proactive investments in hardening critical infrastructure against both man-made and natural occurring hazards can reduce societal risks and also speed economic recovery.

The defining characteristic of wide-area critical infrastructure attack in the 21st century will be infliction of mass casualties without the use of ground troops, air power, or munitions directly against human populations. Deprived of electricity, water, food, heat, and sanitation services, populations concentrated in urban areas will starve, freeze to death, and rapidly die of disease. Without proactive protection of critical infrastructures, people in distress are likely to turn against one another in a fight for survival.

Already there has been some preliminary work to estimate casualties from a wide-area infrastructure attack that would result in long-term blackout of the North American electric grid. Dr. William Graham was chair of the Congressional Electromagnetic Pulse Commission, a study group authorized by the U.S. Congress from 2002 to 2008.[13] Dr. Graham also served as head of the White House Office of Science and Technology Planning and was Presidential Science Advisor. Dr. Graham estimates casualties from a continent-wide electromagnetic pulse attack could be as high as 90%.

A casualty rate of 90% after a wide-area critical infrastructure loss is an extreme prediction indeed. Perhaps the figure in actuality would be 50% or even as low as 10%. But let us remember that there are approximately 324 million residents of the United States. A casualty rate of 10% implies 32 million deaths—far more than all the deaths in all the wars fought by our country.

If these high casualty rates sound unbelievable, I encourage you to engage in a thought experiment. If a densely populated area such as Washington, D.C. lost all electric power, and no outside assistance was available, and people could not evacuate by car because gasoline station pumps were inoperable due to lack of power, and municipal water and sanitation services stopped working, what percent of the population would still be alive after one month?

[13] Under the Defense Authorization Act for FY2016, signed by the President on November 25, 2015, the Congressional EMP Commission is in process of reconstitution. The revived EMP Commission has a mandate to consider both man-made and natural occurring electromagnetic pulses threats; and to consider priority location of defense facilities within states that have strengthened the reliability of their electric grids.

Military-Type Defense of Critical Infrastructure Is Necessary

Within the United States, 99% of military bases rely on the commercial electric grid for their operations, the sole exception being the U.S. Navy's China Lake facility that has a geothermal generator. Were a continent-wide critical infrastructure loss to occur, the U.S. military would rapidly lose its ability to defend. To forestall this outcome, as a society we must examine the current state of military preparation and make adjustments to defend critical infrastructure. Already, the FAST Act requires designation of "Critical Defense Facilities" vulnerable to disruption of electricity supply from the commercial electric grid.

Within the United States, there is presently no effective integration between the defense of critical infrastructure and military authorities. Infrastructure defense is mainly left to civil authorities such as police forces. The Posse Comitatus Act limits the powers of the U.S. Government to use federal military personnel to proactively enforce domestic laws within the United States, including protection against acts which may appear to be criminal in nature.

The Posse Comitatus Act does not apply to National Guard units of the fifty states. Recently there have been proposals to have National Guard units conduct defense against terrorist and foreign cyberattacks. We would welcome these developments.

Large portions of defense budgets are currently allocated to programs designed to fight wars of the 20th century type. For example, the United States and its Allies are projected to spend a lifecycle cost of $1.5 trillion on the Joint Strike Fighter, a weapons system being made increasingly obsolete by unmanned drones and by cruise missiles.

The annual defense budget for the United States is approximately $560 billion. If just 5% of the U.S. defense budget were to be reallocated to critical infrastructure defense, the positive impact on national security would be immense. The alternative—leaving defense of critical infrastructure to individual utilities and local police forces—could leave us with a truly dire outcome.

Cost-Effective Defenses against Grid Attacks and Threats

For any protection of critical infrastructure, costs of protection should be compared with the importance of facilities—including the impact on human populations should defenses fail. Viewed through this metric, one quickly realizes that the money currently spent by utilities on protection of most critical infrastructure is trivial and inadequate. In fact the opposite is true—to save small amounts on construction or maintenance costs, large risks are assumed. A prime example is the remote updating of firmware on critical substation devices by means of the public internet, to save on travel time for maintenance personnel. Unfortunately, the current standard development process at NERC does not use societal cost-benefit analysis as a criterion.

Physical Attack

Because critical infrastructure is widely dispersed, with many unmanned locations, defense against physical attack is challenging. However, the most critical facilities can be cost-effectively

protected. For example, master control rooms for the major electric grid interconnections should have defensible perimeters. Backup locations for master control rooms might be located within military bases. Control centers for natural gas pipelines, telecommunications, and railroads should also have defensible perimeters. In times of imminent threat, police or National Guard units should be dispatched to protect these facilities. Tanker trucks with backup diesel fuel should also be dispatched at the first indication of severe threat or imminent blackout.

The current NERC physical security standard does not apply to Reliability Coordinators or Generator Operators. Reliability Coordinators have sole legal responsibility for coordination of system restoration under the NERC systems of standards; with increasing transfers of power across the seams of control areas, their role is vitally important. The current NERC physical security standard places no specific security requirements on any registered entities but only relies on peer-reviewed plans. Force-on-Force exercises, though required by the Nuclear Regulatory Commission for nuclear power plants, are not mandated for other critical power plants. All of these deficiencies should be remedied by better NERC standards approved through the FERC rulemaking process.

Cyberattack

Presently, electric grid facilities are protected against cyberattack by means of hardware or software that establishes "electronic security perimeters." An entire cybersecurity industry has sprung up to promote and install these "firewall" solutions. This defective defensive philosophy will be invalidated by the first cyberattack on grid infrastructure that results in hundreds, thousands, or millions of deaths. Instead, electric grid facilities should be completely separated from networks connected to the public internet—so-called "air-gapping." Even then, encryption requirements are needed for circumstances in which the "air gap" is breached. With declining costs for fiber optic communications, dedicated communication networks can instead be used for electric grids. Air-gapping combined with broader encryption mandates could be an appropriate protective measure for other critical infrastructure such as pipelines and railroads that supply fuel for electric generation.

Air-gapping should be required by mandatory NERC-FERC standards. NERC should move into compliance with specific provisions of the Energy Policy Act of 2005 by setting standards for cybersecurity protection of communication networks, including encryption of data transmitted over non-proprietary networks.

Electromagnetic Pulse

It is difficult to cost-effectively protect critical infrastructure against electromagnetic pulse attack. For defense against high-altitude nuclear electromagnetic pulse, ballistic missile defense might be the most immediate and cost-effective means. In the long-term, new installations of critical infrastructure can be protected against electromagnetic pulse for approximately 5% of the total system cost—a small amount compared to the risk of losing most of a society's

population. Retrofit protection for electromagnetic pulse is approximately 25% of the total system cost, so delays in establishing mandatory standards will dramatically increase costs.

Solar Storms

It is fortunate that protecting the North American grid against solar storms would be inexpensive. "Neutral ground blocking devices" can protect transformers and other sensitive equipment from malfunction and burn-out. This U.S. government-tested protective equipment is commercially available and costs about $350,000 per facility, plus installation costs. As a rough estimate, about 2,500 locations in the United States with high voltage transformers would need protection against solar storms, costing less than one dollar per year per citizen. The current NERC-proposed standard for solar storm protection does not require hardware protection against solar storms; it only requires paper studies to purportedly show that no protection is necessary. Moreover, the exclusion of Generator Owners and Operators from responsibility for operational responsibilities during solar storms (per Standard EOP-007-1) remains a needless barrier to effective Energy Secretary emergency orders under the FAST Act to protect transformers and other critical equipment at U.S. electric generating facilities.

Partial Protection Is Good Protection

It is a logical fallacy to decide against protecting critical infrastructure because complete protection would be difficult or prohibitively expensive. When the most critical and vulnerable infrastructure is cost-effectively protected, the probability of a successful attack is greatly reduced and the certainty of retaliation against the attackers greatly increased. Significant deterrence against attack thereby results.

Current NERC Standards Process and Rapidly Evolving Security Risks

Questions: How effectively does the current standards process address emerging or rapidly evolving reliability issues? Can Reliability Standards be structured to change quickly for newly-identified security risks or new scientific or engineering analyses (e.g., of geomagnetic disturbances)? If so, how?

Prepared Response: The concept of critical infrastructure as an active battlefield is fundamentally incompatible with the NERC system of standard-setting established by Section 215 and the NERC Rules of Procedure. Moreover, the culture of NERC is to avoid mandatory regulation rather than proactively support military-type defense of critical infrastructure. Common substitutes for mandatory regulation include "information sharing" such as that coordinated by the NERC Electricity Information Sharing and Analysis Center (ES-ISAC); voluntary exercises such as GridEx; and participation in working groups such the Electric Subsector Coordination Council. NERC officials reference these substitutes when testifying why further mandatory measures or remedial legislation are not necessary.

NERC is an organization dominated and effectively controlled by electric utility interests. Seventy percent of NERC members are employed by electric utilities. NERC members regularly

vote to place representatives from large investor-owned utilities in key committee positions. While the NERC Board of Trustees is nominally independent, election of its Trustees is also controlled by NERC members. With this membership and governance structure it should be no surprise that NERC largely operates for the benefit of for-profit electric utilities.

From our perspective as an advocate for the public, NERC persistently conducts its business with the goal of limiting financial liability of utilities for blackouts due to *High Impact, Low Frequency events*. Due to industry lobbying in U.S. state legislatures, electric utilities have been granted safe harbor from liability except in cases of gross negligence. By setting and then applying weak reliability standards—or by not setting standards at all—NERC members have effectively erected legal defenses under the laws of the fifty individual states. One might hypothesize that some electric utilities are so aware of critical infrastructure vulnerabilities and their potential to cause corporate bankruptcy that they have rationally made liability avoidance a foremost priority.

The Ukraine cyberattack exposed the inadequacy of the NERC Critical Infrastructure (CIP) standards for cybersecurity. Even if the Ukraine utilities had followed all of the NERC CIP standards, the cyberattack in Ukraine still would have succeeded. For more information, please see our Motion to Reopen the Evidentiary Record in FERC Docket RM15-14-000.[14]

A significant number of senior utility executives and NERC officials appear to sincerely believe that they are making good and appropriate decisions regarding grid security. Yet the evidence from Ukraine and elsewhere indicates otherwise. How can this be?

For an explanation, we referenced a seminal work on emotional intelligence by researchers Sydney Finkelstein, Jo Whitehead, and Andrew Campbell.[15] These researchers found that executives often make decisions based on intuitive recognition of previous patterns from their own experience or the experience of peers—patterns that are significant because of "emotional tagging."

For example, executives may have experienced blackouts due to severe weather and borne the brunt of public criticism when power is not promptly restored. Alternatively, executives may have seen peer utilities hit by a cascading outage due to an improper setting on protective systems—and seen large fines assessed under the FERC/NERC regulatory system. When prioritizing mitigative actions, these executives may overweight localized and short-term threats that are common, but underweight wide-area, long-term threats that have not yet occurred.

---

[14] Joint Request and Motion to Reopen the Evidentiary Record in Docket RM15-14-000 as Authorized by FERC Rule 716, filed March 29, 2016.

[15] Finkelstein, Sydney, Whitehead, Jo and Campbell, Andrew, "The illusion of smart decision making: the past is not prologue," *Journal of Business Strategy* 2009 30:6 , 36-43. See also Finkelstein, Sydney, Whitehead, Jo and Campbell, Andrew, "Why Good Leaders Make Bad Decisions," *Harvard Business Review*. 2009 Feb;87(2):60-6, 109 and Finkelstein, Sydney, Whitehead, Jo and Campbell, Andrew, *Think Again: Why Good Leaders Make Bad Decisions and How to Keep it From Happening to You*. Boston: Harvard Business Press, 2009. Print.

In fact, much of the NERC system of reliability standards is concentrated on preventing events which commonly occur and therefore can be tracked in their annual "State of Reliability" report. One might reasonably expect that positive presentations of industry metrics would produce feelings of pride and accomplishment at both NERC and FERC. But overemphasis of such metrics can lead to bad decision making for rare but catastrophic events.

Additional FERC authority to unilaterally set and enforce electric reliability standards would be one solution to deficiencies in the NERC-FERC standard-setting and approval process.

Replacement of Large Power Transformers after an Emergency

Questions: Is progress being made on standardization and transportation of transformers to facilitate timely replacements after an emergency? Are there actions the Commission should consider to encourage progress?

Prepared Response: There are currently no electric reliability standards for sparing or rapid replacement of large power transformers. Utility action under "best practices" has been lackluster and inadequate. For example, the U.S. Department of Homeland Security financed the development of a prototype "Recovery Transformer" (RecX) and arranged for it to be deployed and tested in an operational grid in Texas. According to media reports, several years later not a single production unit had been put into spare inventory. The Grid Assurance industry cooperative for spares has likewise been launched with great fanfare. However, because there will be no public disclosure of adequacy of spares, it is possible this industry initiative is intended mostly to forestall legislation or mandatory standards. For more information, please see our filing on FERC Docket EL-15-76.[16]

Under the FAST Act approved in December 2015, specifically Section 61004, the Secretary of Energy has a mandate to develop a Strategic Transformer Reserve. Further, under the new Section 215A of the Federal Power Act, authorized by the FAST Act, the Secretary of Energy will have authority to authorize cost-recovery for orders issued during energy emergencies that may last up to 15 days, or an extended set of 15-day emergency periods.

The FERC Commissioners and Staff should welcome, as we do, these new emergency authorities and cost-recovery opportunities vested in the Secretary of Energy.

We would be remiss, however, if we did not ask the Commissioners and Staff to recognize that the protection of existing high voltage transformers and the placement of reserve transformers near large generating facilities remain "best buys." Generally speaking, preventing transformer damage and deploying geographically proximate transformer spares are safer options than dependency upon shared inventory that is in limited numbers and difficult to transport quickly.

To protect an expensive transformer from total loss, and the need for long-lead replacement that may include formidable transportation obstacles, the Commission should welcome "best

[16] Foundation for Resilient Societies, Inc. Motion to Intervene re: Grid Assurance, LLC, filed July 9, 2015.

practices" that include cost-recovery for protective equipment such as neutral ground blockers that may exceed the minimum required in standards that NERC sets and FERC approves.

We urge the Commission and its FERC staff to strengthen coordination with the Department of Energy to identify complementary "best buy" investments in electric grid resiliency. Recently, Resilient Societies has urged the Commission to build upon a Commission practice of enabling cost-recovery for "best practices" that includes purchase of "blackstart" generation and transmission capabilities, and reactive power capabilities. Specifically, we have urged the Commission to welcome applications for cost recovery for neutral ground blockers to protect high voltage transformers and related equipment to better cope with solar geomagnetic disturbances.[17]

Because the average installed life of large power transformers is approximately 40 years, original transport methods may no longer be available. For example, railroad spur lines may have been taken out of service. Transportation planning for large power transformer replacement should be done in advance of emergencies.

Also because the average installed life of large power transformers is approximately 40 years, detailed data on transformer design characteristics may have been lost. In some cases, the only data still available is so-called "nameplate data." When transformer design data is available, it may be kept only in electronic records that would be hard to access during a blackout. Standards are needed for record-keeping on large power transformers. In some cases, this design data should be communicated to government authorities, such as the Department of Energy, in advance of emergencies.

The Commission's authority to enable cost recovery under Sections 205 and 206 of the Federal Power Act continues in force, and complements the new authority for cost recovery for emergency actions vested in the Secretary of Energy under the Federal Power Act's new Section 215A, part of the FAST Act. After many years of waiting for utilities to implement "best practices," it would now be appropriate for FERC to issue a *sua sponte* order for electric reliability standards for record-keeping, sparing, transportation planning, and rapid installation of large power transformers. And the Commission should establish cost recovery procedures through consideration of FERC Docket RM15-11-000.

Research of Electromagnetic Pulse Effects on Electric Grids

Questions: What is the status of research on whether or how electromagnetic pulses might affect the grid? What additional research would help address any uncertainties?

Prepared Response: The long rise-time or "E3" electromagnetic pulse is common to both nuclear EMP and naturally-occurring solar storms. Research on protection from solar storms has been greatly hindered by the withholding of operational Geomagnetically Induced Current

[17] See the March 15, 2016 Filing of the Foundation for Resilient Societies in FERC Docket RM15-11-000, citing many FERC precedents for cost-recovery, with the burden of proof upon the Applicant per Federal Power Act sec. 205.

(GIC) data by electric utilities. Utilities are also withholding data on failures of large power transformers during and shortly after solar storms. Some of this data is contained in the NERC Generating Availability Data System (GADS) and Transmission Availability Data System (TADS) databases. Mandatory provision of data by NERC and electric utilities to both the Commission and to appropriate research organizations could advance research and strengthen opportunities for design and acquisition of protective equipment that would work to protect against both man-made and naturally-occurring electromagnetic pulse hazards.

Compliance with NERC CIP and PRC Standards

Questions: The CIP and PRC standards continue to be among the most-often violated Reliability Standards. What efforts are being made, or should be made, to improve compliance with these particular standards?

Prepared Response: The fundamental structure of the NERC CIP Standards that rely on so-called Electronic Security Perimeters and hardware/software firewalls is complicated, unsound, and prone to violation. A more simple solution would be "air-gapping" combined with encryption requirements extending to electric substations. Compliance could be more easily monitored and violations would likely decrease.

As we learn from the Ukrainian electric grid takedown, it is essential to develop standards to remove malware and vulnerable firmware from the U.S. electric grid. Once the grid has experienced a partial takeover by a foreign power, the time to verify the restoration of control system integrity may be extended in time. For example, four months after the attack, Ukrainian distribution utilities continue to operate with manual controls instead of the usually reliable automated control systems. Therefore, the Commission needs to concentrate upon more functionally appropriate cyber-protection standards than CIP5/6, including a duty to remove identified families of malware from the Bulk Power System.

Challenges for Democratic and Capitalist Societies

Every day, the citizens of America are exposed to existential threats caused by inadequate protection of critical infrastructure, especially the electric grid. However, the history of budgetary allocations and legislative reform in democracies shows that high-impact events that have not yet occurred are often assumed by political leaders to be too improbable or too expensive against which to defend. Constituents may erroneously assume that elected and appointed officials have diligently studied infrastructure vulnerabilities and prepared for the common defense or, alternatively, constituents may be too busy with their daily lives to give much thought to potential calamities outside their direct experience.

Critical infrastructure in the United States is principally owned and operated by private companies. In our experience, at least some senior executives of electric utilities have given thought to infrastructure vulnerabilities and are acutely aware about lack of protective

measures. However, the profit incentive, as expressed through normal operation of capital markets, provides inadequate justification to protect from attacks or disasters that occur so infrequently that they probably will not happen during the tenure of current managers. Moreover, executives at private companies can understandably have the attitude that defense of societies is a government responsibility apart from their day-to-day operations.

Conclusion

While North America has not yet experienced a long-term, wide-area grid security event, the public is growing increasingly aware of threats to the electric grid and other infrastructure. Critical infrastructure can be cost-effectively defended, but government policymakers, industry stakeholders, and other involved parties need to reexamine assumptions and established processes in the context of evolving threats.

The Commission needs to recognize, as the Congress has signaled through recent legislation, that reliability metrics derived from conventional weather and other common outage causes fail to prepare us for high impact consequences of prolonged blackouts. By embracing contingency modeling for extreme events that have not yet occurred, and by seizing the opportunities resulting from recent legislation, the Commission can strengthen electric reliability and societal resilience.

By holding this hearing and providing an opportunity for our testimony, FERC has shown leadership in considering whether the public is adequately protected from both naturally-occurring and man-made threats to a secure and reliable electric grid.

Thank you for the opportunity to testify. I look forward to any questions.

Appendix 2—Testimony of Resilient Societies to Canadian Parliament

Testimony of Thomas S. Popik, Chairman
Foundation for Resilient Societies
before the
Canadian Standing Senate Committee on National Security and Defence
Monday, April 18, 2016

My name is Thomas Popik, and I am chairman of the Foundation for Resilient Societies, a non-profit group dedicated to the protection of critical infrastructure, including the electric grid, within North America.

Before I get into the substance of my remarks, I would like to say that I am deeply appreciative of the opportunity to testify before your Senate Committee on National Security and Defence. My personal involvement in the defense of Canada goes back to the early 1980's, when I was a young U.S. Air Force officer assigned to the upgrade of the Distant Early Warning Line (DEW Line), a string of 33 radar sites operated at the northern-most reaches of the North American land mass. When I was a 2nd Lieutenant in the U.S. Air Force, my first supervisor and mentor was a major in the Royal Canadian Air Force.

I have had the privilege to see much of your great country, including not only the major metropolitan areas of Toronto, Montreal, and Vancouver, but also more remote areas such as Yellowknife in the Northwest Territories, Cambridge Bay on Victoria Island, and vast expanses of Baffin Island. In preparation for this hearing, I have also taken time to familiarize myself with the electricity generation, transmission, and distribution system for Canada and how it is operated and regulated.

Background on Resilient Societies

The directors and staff of Resilient Societies include some of North America's foremost experts on critical infrastructure protection. Through the public docket process and other means, we

provide policy advice to federal agencies within the United States, including the principal regulator of the U.S. bulk power system, the Federal Energy Regulatory Commission (FERC).

Resilient Societies regularly participates in standard-setting for electric reliability at the North American Electric Reliability Corporation (NERC), an industry self-regulatory body that sets electric grid reliability standards for both the United States and Canada. We have expended thousands of hours of professional staff time participating in the NERC standard-setting process, including attending in-person meetings of key committees and directly interacting with senior NERC officials. For some important standard-settings at NERC, we have been the only public interest group participating. As a result, my group has gained significant insight into the security and vulnerabilities of the North American electric grid and other critical infrastructure. For more information about Resilient Societies, please see on our website at www.resilientsocieties.org.

Key Infrastructure Threats

According to our risk assessments, four threats have potential to take down electric grids and other interdependent infrastructures for months or years, causing catastrophic military, economic, societal, and environmental impacts: physical attack, cyberattack, electromagnetic pulse, and solar storms. All of these threats have the potential for a long-term impact over a geographic area so widespread that no significant outside assistance would be available. For some threat scenarios, immediate impacts could be continent-wide.

Physical Attack

On April 16, 2013 unknown parties attacked the Metcalf substation in San Jose, California, a critical electric grid facility. These attackers first cut telecommunications lines to the substation and then shot out the radiators for 17 of 21 extra high-voltage transformers. The attackers ceased their assault just one minute before police arrived on the scene.

Fortunately, the attackers had missed cutting one last telecommunications cable, allowing system operators to monitor rising temperatures in the transformers. The operators rerouted electricity loads before the transformers overheated and exploded. Had just one more

transformer been shot out, or had the system operators not been able to intervene, a catastrophic blackout would have occurred.

While insiders in the electric utility industry quickly understood the gravity and implications of the Metcalf substation attack, media attention at the time was scant. One reason may have been the distraction of the Boston Marathon bombing, which had occurred just 13 hours before the Metcalf attack.

The Metcalf substation supplies the majority of electric power for Silicon Valley and San Francisco, one of the greatest concentrations of high-technology companies in the world. Had the attack fully succeeded, a cascading outage would have likely impacted much of northern California. Large power transformers are principally manufactured in Europe and Asia with lead times of one to two years, have few available spares, and are difficult transport. Had the transformers been permanently damaged, the region would have experienced severe power shortages lasting days, weeks, or months.

In February and March 2014, front page stories in the *Wall Street Journal* disclosed the national importance of the Metcalf substation attack. Truly, this attack was a wake-up call. One of the key sources for these stories was none other than the prior FERC chairman, Mr. Wellinghoff. According to an engineering analysis performed by FERC and leaked to the Wall Street Journal, a coordinated attack on just nine grid substations could bring down most of the North American electric grid for more than a year.

Cyberattack

On December 23, 2015, a sophisticated cyberattack struck the Ukrainian electric grid, blacking out approximately 225,000 electricity customers. This well-executed attack took over grid operators' control stations, deleted data on hard drives, remotely opened circuit breakers at more than 120 electric substations, and damaged substation equipment necessary for rapid power restoration. Cybersecurity experts have long predicted, and demonstrated via the Aurora test at Idaho National Laboratory in the United States, that a cyberattack can cause a long-term grid blackout by permanently damaging generators and other equipment. Events in the Ukraine

move the risk of deliberate cyberattack on critical infrastructure from a theoretical possibility to a demonstrated reality.

Electromagnetic Pulse

A high-altitude electromagnetic pulse attack would damage sensitive computer chips used in control systems for the electric grid. Large and hard-to-replace power transformers would also be permanently disabled. The result could be a continent-wide blackout lasting months or years. In fact, such a blackout might be non-recoverable.

Cheap and easy-to-assemble devices the size of a suitcase or small cargo van can also produce localized electromagnetic pulse. If terrorists or foreign powers were to place such devices close to grid substations and control rooms, and simultaneously operate these devices, a continent-wide blackout could also occur.

In 2008, the U.S. Congressionally-authorized Electromagnetic Pulse Commission determined that "EMP is one of a small number of threats that can hold our society at risk of catastrophic consequences...It has the capability to produce significant damage to critical infrastructures and thus to the very fabric of US society, as well as to the ability of the United States and Western nations to project influence and military power."

Solar Storms

Because of its northern latitude, Canada is particularly exposed to the threat of blackout from severe solar storms. There are numerous ways that solar storms could cause wide-area, catastrophic blackouts. High voltage transformers in critical locations could melt down, catch fire, or explode. The voltage of the grid could collapse. Generators could overheat and fail. And when the storm hits satellites in orbit, it could interrupt the Global Positioning System (GPS) timing signals vital for wireless networks increasingly used for grid substation communications and control. Let us remember that a relatively small solar storm already caused a blackout for the entire province of Quebec in just 92 seconds in March 1989.

Critical Infrastructure Will Be a 21st Century Battlefield

War in the first half of the 20th century was characterized by battles between massed ground and naval forces supported by air power. In the second half of the 20th century, wars were increasingly fought against terrorists and insurgencies in countries far from North America.

Already in the 21st century, we see attacks against critical infrastructure being used as an instrument of war. Recent examples include a physical attack against high voltage transmission lines in the Crimea and a cyberattack against electric distribution facilities in Ukraine. Within the next decade, I fear that North America will experience its first wide-area infrastructure attack by terrorists or foreign powers.

Already within Canada, domestic terrorists attacked high voltage transmission lines of Hydro Quebec in December 2014, by means of an airplane. This attack caused an immediate blackout for several hundred thousand people and reversed the normal flow of power from Canada to the United States. In early 2015, I was present at a meeting of system operators where the technical forensics of this incident were reviewed.

When terrorists launch an attack directly against humans, as one did in October 2014 on Parliament Hill, it is an assault against the idea of an open and free society—and a tragedy for the individuals directly affected. Were terrorists or a foreign power to launch an effective infrastructure attack against Canada and the United States, it could threaten the continued existence of these countries—and result in millions of deaths. Conversely, proactive investments in hardening critical infrastructure against both man-made and natural occurring hazards can reduce societal risks and also speed economic recovery.

The defining characteristic of wide-area critical infrastructure attack in the 21st century will be infliction of mass casualties without the use of ground troops, air power, or munitions directly against human populations. Deprived of electricity, water, food, heat, and sanitation services, populations concentrated in urban areas will starve, freeze to death, and rapidly die of disease. People will turn against one another in a fight to survive just a bit longer.

Already there has been some preliminary work to estimate the casualties from a wide-area infrastructure attack that results in long-term blackout of the North American electric grid. Dr. William Graham was chair of the Congressional Electromagnetic Pulse Commission, a study group authorized by the U.S. Congress from 2002 to 2008. Dr. Graham also served as head of the White House Office of Science and Technology Planning and was Presidential Science Advisor. Dr. Graham estimates casualties from a continent-wide electromagnetic pulse attack could be as high as 90 percent.

A casualty rate of 90 percent after a wide-area critical infrastructure loss is an extreme prediction indeed. Perhaps the figure in actuality would be 50 percent or even as low as 10 percent. But let us remember that there are approximately 350 million residents of Canada and the United States. A casualty rate of 10 percent implies 35 million deaths—far more than all the deaths in all the wars fought by both countries.

If these high casualty rates sound unbelievable, I encourage you to engage in a thought experiment. If a densely populated area such as Toronto lost all electric power, and no outside assistance was available, and people could not evacuate by car because gasoline station pumps were inoperable due to lack of power, and municipal water and sanitation services stopped working, what percent of the population would still be alive after one month?

Military Defense of Critical Infrastructure

Within the United States 99% of military bases rely on the commercial electric grid for their operations, the sole exception being the U.S. Navy's China Lake facility that has a geothermal generator. Were a continent-wide critical infrastructure loss to occur, the militaries of Canada and the United States would rapidly lose their ability to defend us.

To forestall this outcome, we must examine the current state of military preparation and make adjustments to defend critical infrastructure. Within the United States, there is presently no effective integration between the defense of critical infrastructure and military authorities. Infrastructure defense is mainly left to civil authorities such as police forces. The Posse Comitatus Act limits the powers of the U.S. Government to use federal military personnel to

proactively enforce domestic policies within the United States, including protection against acts which may be criminal in nature.

The Posse Comitatus Act does not apply to National Guard units of the fifty states. Recently there have been proposals to have the National Guard units conduct defense against terrorist and foreign cyberattacks.

Large portions of defense budgets are currently allocated to programs designed to fight wars of the 20th century type. For example, the United States and its allies are projected to spend a lifecycle cost of $1.5 trillion (US) on the Joint Strike Fighter, a weapons system being made increasingly obsolete by unmanned drones and cruise missiles. If Canada continues to participate in the Joint Strike Fighter program, the estimated lifecycle cost would be $46 billion.

The annual defense budget for the United States is approximately $560 billion (US). The annual defense budget for Canada is approximately $19 billion. If just 5 percent of the defense budgets of both nations were reallocated to critical infrastructure defense, the positive impact on national security would be immense.

The alternative—leaving defense of critical infrastructure to local governments and police forces—could leave us with a truly dire outcome. If a critical infrastructure failure were to cause a loss of most of the population, an invading army could feasibly take control of key parts of North American land mass. There would be ample incentive for some foreign powers to do so, because Canada and the United States have immense quantities of natural resources that could be extracted and shipped overseas via the surviving rail, waterway, and port infrastructure. Does this scenario sound so farfetched as to not be worth consideration? The course of human history—including colonization of continents for their natural resources—teaches us otherwise.

Cost-Effective Protective Measures

For any protection of critical infrastructure, costs of protection should be compared with the importance of facilities—including the impact on human populations should defenses fail. Viewed through this metric, one quickly realizes that the money currently spent by utilities on protection of most critical infrastructure is trivial and inadequate. In fact the opposite is true—

to save a few dollars on construction or maintenance costs, large risks are assumed. A prime example is the remote updating of firmware on critical substation devices by means of the public internet, to save on travel time for maintenance personnel.

Physical Attack

Because critical infrastructure is widely dispersed, with many unmanned locations, defense against physical attack is challenging. However, the most critical facilities can be cost-effectively protected. For example, master control rooms for the major electric grid interconnections should have defensible perimeters. Backup locations for master control rooms might be located within military bases. Control centers for natural gas pipelines, telecommunications, and railroads should also have defensible perimeters. In times of imminent threat, police or troops should be dispatched to protect these facilities.

Cyberattack

Presently, electric grid facilities are protected against cyberattack by means of hardware or software that establishes “electronic security perimeters.” An entire cybersecurity industry has sprung up to promote and install these “firewall” solutions. This defective defensive philosophy will be invalidated by the first cyberattack on grid infrastructure that results in hundreds, thousands, or millions of deaths. Instead, electric grid facilities should be completely separated from networks connected to the public internet—so-called “air-gapping.” With declining costs for fiber optic communications, dedicated communication networks can instead be used for electric grids. Air-gapping could be an appropriate protective measure for other critical infrastructure such as pipelines and railroads.

Electromagnetic Pulse

It is difficult to cost-effectively protect critical infrastructure against electromagnetic pulse attack. For defense against high-altitude nuclear electromagnetic pulse, ballistic missile defense might be the most immediate and cost-effective means. In the long-term, new installations of critical infrastructure can be protected against electromagnetic pulse for approximately 5 percent of the total system cost—a small amount compared to the risk of losing most of a society’s population.

Solar Storms

It is fortunate that protecting the North American grid against solar storms would be inexpensive. “Neutral ground blocking devices” can protect transformers and other sensitive equipment from malfunction and burn-out. This U.S. government-tested protective equipment is commercially available and costs about $350,000 per installation. As a rough estimate, about 300 locations in Canada with high voltage transformers would need protection against solar storms.

Partial Protection Is Good Protection

It is a logical fallacy to decide against protecting critical infrastructure because complete protection would be difficult or prohibitively expensive. When the most critical and vulnerable infrastructure is cost-effectively protected, the probability of a successful attack is greatly reduced and the certainty of retaliation against the attackers greatly increased. Significant deterrence against attack thereby results.

Challenges for Democratic and Capitalist Societies

Every day, the citizens of Canada and the citizens of all of North America are exposed to existential threats caused by inadequate protection of critical infrastructure, especially the electric grid. However, the history of budgetary allocations and legislative reform in democracies shows that high-impact events that have not yet occurred are often assumed by political leaders to be too improbable or too expensive against which to defend. Constituents may erroneously assume that elected officials have diligently studied infrastructure vulnerabilities and prepared for the common defense or, alternatively, constituents may be too busy with their daily lives to give much thought to potential calamities outside their direct experience.

Critical infrastructure in North America is principally owned and operated by private companies. In our experience, senior executives of major infrastructure operators have given much thought to infrastructure vulnerabilities and are often acutely aware about their lack of proactive steps for protection. However, the profit incentive, as expressed through normal operation of capital markets, provides inadequate justification to protect from attacks or disasters that occur so infrequently that they probably will not happen during the tenure of current managers. Moreover, private companies understandably have the attitude that defense of societies is a government responsibility apart from their day-to-day operations.

Deficiencies in the Current Regulatory System

Electric grid security in the United States and Canada is governed by a common set of regulatory standards. Standards are set by North American Electric Reliability Corporation, a self-regulatory body set up in the aftermath of the 2003 Northeast Blackout. NERC has been given authority to regulate electric utilities legislation passed by the U.S. Congress in 2005. Previously, NERC was a trade association located in Princeton, New Jersey.

NERC is an organization dominated and effectively controlled by electric utility interests. Seventy percent of NERC members are employed by electric utilities. NERC members regularly vote to place representatives from large investor-owned utilities in key committee positions.

While the NERC Board of Trustees is nominally independent, their election is also controlled by NERC members. With this membership and governance structure it should be no surprise that NERC acts principally to further the goals of for-profit electric utilities.

From our perspective as an advocate for the public, NERC persistently conducts its business with the goal of limiting financial liability of utilities for blackouts. Due to industry lobbying in U.S. state legislatures, electric utilities have been granted safe harbor from liability except in cases of gross negligence. By setting and then following weak reliability standards—or by not setting standards at all—NERC members have effectively erected legal defenses under the laws of the fifty individual states that comprise the United States. One might hypothesize that some electric utilities are so aware of critical infrastructure vulnerabilities and their potential to cause corporate bankruptcy that they have rationally made liability avoidance a foremost priority.

Because NERC's electric reliability standards must be approved by governments before becoming enforceable, there are nominal checks on its behavior. By U.S. law, our Federal Energy Regulatory Commission must assure that NERC standards are "in the public interest." In practice, the public interest often is judged by FERC to coincide with corporate interests. The provincial governments of Canada also have a role in oversight of NERC. However, in our experience, the influence of provincial governments on the NERC standard-setting process is minimal.

Conclusion

While North America has not yet experienced a long-term, wide-area infrastructure outage, the public is growing increasingly aware of threats to the electric grid and other infrastructure. Critical infrastructure can be cost-effectively defended, but government policymakers and the regulatory systems they have established have not risen to the challenge. By holding this hearing, your Committee has shown leadership in reinforcing public awareness of critical infrastructure threats. We hope that you might take the next step by proposing effective means for the national defense against such attacks.

Thank you for the opportunity to testify. I look forward to any questions.