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[1] and their replacement with gas-fired plants dependent on just-in-time fuel delivery through long pipelines[2]
- 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[3]
- 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

---

[1] 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 .

[2] 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#.

[3] 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.

- Closure or minimization of blackstart resources to comply with cybersecurity standards or environmental regulations

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[4]
- 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

[4] 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.[5]

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

[5] 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.[6] 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

[6] 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.

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-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.[7]

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.[8] 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

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

[8] 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.

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.

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.[9]

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

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

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 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.[10]

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.

[10] 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.

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 (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.