UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Reliability Technical Conference **Docket No. AD17-8-000**

Testimony of Dr. George H. Baker, Senior Advisor to the Congressional EMP Commission

At the June 22, 2017 Reliability Technical Conference
Submitted to FERC on June 12, 2017

Many thanks to Chairman LaFleur and the other FERC commissioners for this opportunity to share my thoughts on assuring electric power grid reliability. My name is George Baker and I have spent most of my professional career protecting the U.S. military from the nuclear electromagnetic pulse (EMP). At the Defense Nuclear Agency and successor Defense Threat Reduction Agency (DTRA), I managed the development of the military standards used to protect Department of Defense (DoD) systems and performed vulnerability assessments of critical military facilities and supporting infrastructure. In my second career as an academic, I directed James Madison University's Institute for Infrastructure and Information Assurance and developed courses on complex infrastructure systems and how they fail, and nuclear energy technology.

As in years 2001-2008, I again serve as a Senior Advisor to the Congressionally-mandated Commission to Assess the Threat to the United States of Electromagnetic Pulse (EMP) Attack. The current mandate of the Commission includes assessments of "progress" made by federal departments, agencies, and civil infrastructure institutions in protecting against EMP, GMD, cyber, and physical attacks – including but not limited to the bulk power electric power system. My appearance today substitutes for a presentation by Mr. Earl Gjelde, an EMP Commissioner, who was unable to attend today's Reliability Technical Conference.

The nature of EMP, cyber, and physical threats (here referred to as "triple threat" contingencies) to our grid are severe, to be sure. We include within the scope of 'EMP' both natural occurring solar storms and the more energetic man-made EMP hazards. Bounding consequences could include risk measurement units of millions of casualties (EMP Commission), trillions of dollars (Lloyds of London), and, dents in the history of civilization

(Center for Policy on Emerging Technology). The good news is that well-known engineering solutions are available to counter these threats.

I will use my time this afternoon to offer a vision for a future in which our electric power systems will be able to operate through or quickly recover from catastrophic failure due to EMP, cyber, and physical attacks. I have discussed this vision with members of the electric power industry, and prominent EMP/cyber/physical protection advocates who find it to be supportable and actionable. There is much we can agree on since we all want a grid that is immune to long-term outages.

Here is the vision:

1. Industry and Government working together to achieve an electric power grid resilient to combined EMP/cyber/physical attacks
2. Electric utilities able to recapture costs associated with physical protection of the grid
3. A unified model of the national grid effects and recovery steps verified by shared data to enable identification of the most critical system failure points leading to a prioritized list of actionable and affordable protections.
4. A coordinated national-level Blackstart plan and resources that are exercised on a regular basis.
5. A single accountable national authority given overall responsibility for electric power grid (EPG) protection architectures and standards. Uniform national assessment and protection guidelines issued and enforced by the national EPG protection authority.
6. Capital investments and cost recovery decisions reviewable and approvable by FERC for the bulk electric system and by state regulators for the distribution system.

I will address these vision elements in sequence:

1. Industry and Government working together to achieve comprehensive electric power grid resiliency to EMP/cyber/physical attacks.

Public-private partnerships will be essential to protecting our grid. U.S. high-consequence natural disasters have clarified the importance of government collaboration with industry. The resources owned and controlled by American industry dwarf those available to local, state, and even federal government departments. Better agreements and incentives to bring the full capabilities of the electric power industry into the national preparedness and response arena will be indispensable in effectively protecting the grid and responding in triple-threat contingencies. There are already, as we speak, good examples of public-private partnerships in the discipline of multi-hazard grid resiliency including the InfraGard EMP Special Interest Group and their table top exercises and recent publication, “Powering Through: From Fragile

Infrastructures to Community Resilience." This guidebook was prepared with inputs from federal government, state government, the electric power industry, academia, and system developers, and independent consultants. A threat composite diagram from the guidebook is included in Figure 1.

Several public-private table top exercises have occurred including events at the Army War College, the National Defense University, the Johns Hopkins Applied Physics Laboratory, the National Association of Regulated Utility Commissioners, and the National Guard Association of the United States. Of special note, a public-private cooperative effort is taking shape with Duke Energy working with state and local infrastructure service providers and emergency responders at Lake Wylie in a pilot EMP protection demonstration project in the Carolinas, in coordination with Ambassador Hank Cooper.

Equipment at Risk	EMP	Solar Storm	Cyber	Physical Attack	Radio Frequency Weapons
Transformers	R	R	R – Y	R	R
Generator Stations	R	G	R	R	R
SCADA / Industrial Controls	R	R	R	R	R
Utility Control Centers	R	R	R	R	R
Telecommunications including cell phones	R	R	R	Y	Y
Radio Emergency Communications	R	P	Y	Y	Y
Emergency SATCOM Communications	R	P	Y	Y	Y
Internet	R	R	R	Y	Y
GPS	R	P	Y	Y	Y
Transportation	R	Y	Y	Y	Y
Water	R	Y	R – Y	Y	Y

Legend: Red = direct permanent effects. Yellow = Cascading effects if no backup power. Pink = temp. effect (.5- 36 hours) assuming backup power. Gray = direct effects uncertain.

Figure 1. Threats to the Electric Power Grid and Supporting Infrastructures

It is important to note that, for the grid to be resilient, we must also identify and include infrastructures directly supporting the electric grid such as communication, fuel sources, transportation, and water supply in our protection programs. The Lake Wylie project and the InfraGard programs do this. A cost study by the Foundation for Resilient Societies determined that, with careful prioritization, grid-supporting infrastructure protection costs are manageable.

I contend that, with respect to the grid, because of its exposure and ease of attack, we must create partnerships that address multiple hazards. Stove-pipe attention to single threats necessitate needless and too costly redundancies in system protection. DTRA's blue ribbon assessment programs have found that all hazards protections are imminently doable – that

once key "single-point failure" locations are identified, protection of these against multiple hazards is straightforward. And it is important that EMP is not ignored – it is problematic that EMP was not listed among the DHS top 100 threats[1] and that current GMD efforts neglect to address identical vulnerabilities and protection measures associated with the EMP waveform.

Due to its 50+ year learning from actual EMP specification, design, and implementation experience, DoD participation is crucially important. The U.S. military already has EMP protection approaches that are tested and well understood that can be translated directly to electric power grid control facilities and supervisory control and data acquisition electronics and networks. For more than a half-century, high profile military command, control, and computer systems for nuclear deterrence and response have been protected against EMP attacks. Regional civilian grids have not yet been designed for this capability, nor have most commercial microgrids.

The inadequate sharing of DoD-provided insights has led DOE and the Electric Power Research Institute (EPRI) to redefine EMP environments and system protection criteria which will greatly confuse the playing field. As a case in point, EPRI's recent E3 study is using an environment criteria that is well below corresponding DoD transmission and distribution transformer protection requirements. It would be both illogical and imprudent to adopt weaker EMP protection standards for the commercial electric grid, when about 98 percent of military facility power depends upon the commercial power grid.

It is worth stating that engineers (power, communication, computer, materials, and structures) can solve triple threat protection problems, as they have for DoD, if we give them the resources, well-posed technical performance requirements, and let them loose.

2. Electric utilities able to recapture costs associated with physical protection of the grid.

My colleague, Tom Popik, has addressed this part of the vision in his FERC submission and I refer you to his presentation. A persistent barrier to approval and implementation of effective grid reliability standards has been inadequate cost recovery opportunities. Potential mechanisms for cost recovery include FERC-approved tariffs, federal tax credits, and appropriations for cost sharing, as with the Smart Grid Investment Grant program of 2010-2015. Under deregulation, competition has had an opposing effect on reliability. The adage, "private efficiency leads to public vulnerability," applies here.[2] Better designed electricity markets with incentives reducing multi-hazard risk of catastrophe would have a major effect on grid resiliency.

Important financial incentives for grid protection can also be provided by the insurance industry. Insurance providers could set basic resilience standards as part of their terms of

[1] Fortunately, Section 1913 of the National Defense Authorization Act for FY 2017 encourages development of a DHS strategy for critical infrastructure resilience, including both solar storm and man-made EMP hazards.
[2] P. Auerswald et al, Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability, Cambridge University Press, 2006.

coverage for utilities companies regarding long-term outage-producing events. Existing public-private partnerships in the United States and Europe that divide the risks of potential terrorist attacks between public and private sectors should be used as a model for cooperation between government and utilities to protect critical infrastructures. To help the insurance industry create proper models for pricing risk associated with possible electromagnetic (EM) events, these solutions will require access to the electric industry's historical data bases on grid failures due to GMD, ground faults, and switching transients.

3. A unified model of the national grid effects and recovery steps verified by shared data to enable identification of the most critical system failure points leading to a prioritized list of actionable and affordable protections.

Grid vulnerabilities can be reduced by hardening the electric grid and by executing smart shutdowns if warning is available. Identification of the most critical system failure points can enable a list of cost-effective protection priorities. Smart, timely reconstitution of the grid following a planned or unplanned shut-down is an equally important piece of the planning process. All of these – prioritized system hardening, smart shutdown and smart reconstitution – will require improved multi-threat grid modeling. A major objective of modeling will be the identification of the most critical system and network failure points to enable generating the list of system protection priorities. DOE has included provisions for improved grid modeling in its recently issued EMP Action Plan.

Several models of the grid exist at diverse locations including the National Infrastructure Simulation and Analysis Center (NISAC), the University of Illinois, and FERC. Many electric utilities have models for their networks. These models have been developed to simulate and better understand grid failure mechanisms. The NISAC model is perhaps the most comprehensive in scope, having been developed for the composite national grid. However, the NISAC model remains limited in its ability to handle multiple threats. Models to assist in determining the best sequence of recovery steps following a major grid collapse are not yet available but should be developed collaterally with grid failure models since they involve the reverse processes.[3] Modeling of electric grids under scenarios of equipment damage and broken connectivity will be important for emergency planning.

Model development would be greatly abetted if industry historical data bases are made available for model validation purposes. Since the simulators used for EMP tests have exposure areas that can accommodate single locations only (i.e., network node systems such as generators, transformers, and control rooms), the ultimate assessment of EMP effects on the grid must rely on modeling the behavior of the larger grid networks by incorporating single node test data. Note that GMD effects, analogous to EMP/E3 effects and consequences, are

[3] NERC and FERC are to be commended for their January 2016 FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans."

provided by strong solar storms so we can get network-wide validation of GMD and EMP/E3 models from system effects observations and GIC/electromagnetic field measurements. Many existing models have not been experimentally validated. Models verified by test-to-failure data are needed to gain confidence in prediction of EMP/GMD impacts and the effectiveness of grid protection options.

Empirical validation of models is very important for confidence building. Electromagnetic system effects and hardening requirements are tried and true for communication, computer, and control electronics due to DoD protection installation and test programs and standards development. We have yet to perform "test-to-failure" model validation for electromagnetic effects (EMP and GMD) on large transformers and generator stations. Model development based on testing of cyber attack vulnerabilities of industrial control systems is also needed.

4. A coordinated national-level blackstart plan and implementation resources that are exercised on a regular basis.

Although NERC regional operators have blackstart plans for limited blackout contingencies, there is presently no national plan addressing restoring the grid following a large-scale, "long-term outage" (LTO) blackout contingency. The LTO phenomenon has been defined by the President's National Security Telecommunications Advisory Panel (NSTAC) as an interruption of electricity and/or communications for a period long enough, and over a large enough geographic region, to hamper providing electric power and communications even by alternative means. An LTO contingency has not yet occurred in North America. In some scenarios, the entire continent can be affected with no unaffected region of the country to reliably provide mutual assistance to severely affected areas. In addition, EMP and GMD effects may take out communication and data networks that have been available for recovery coordination during more limited blackouts. Triple-threat blackout contingencies will be particularly challenging, given that large numbers of bulk power system generation and transmission equipment may be damaged. In these circumstances, existing regional blackstart plans may not be adequate.

A North American blackstart plan is needed to identify utilities that are most likely to sustain generator operation (e.g., high complement of black-startable hydroelectric plants) or can most rapidly revive high capacity generator operations. As an example, in the event of a North America-wide blackout, New England grids can be more easily divided into smaller grid islands and are richer in hydroelectric plants, thus they may be restarted more quickly and provide the energy basis for restarting other parts of the grid. Hydroelectric plants are most prevalent in the Northeast and Northwest U.S.

Under existing grid reliability standards, electric utilities are required to establish blackstart equipment and procedures. Hydroelectric plants, coal-fired plants, and gas-fired plants are commonly used for blackstart. "Cranking paths" are then employed between blackstart plants and other generation facilities such as nuclear plants. It will be important to protect key blackstart equipment against EMP and cyber-attack effects. The blackstart process requires that

generators have adequate loads, which means that a minimum set of load systems will need to be protected or rapidly restored. It is vital to restart the grid as quickly as possible.

Local blackstart plans have been developed involving adoption of a “grid islanding” architecture and a priority ranking within an inventory of “grid islands” including key power plants to be restarted following a major grid blackout. Initially, the grid blackstart occurs within isolated “grid islands.” Once the grid islands are functional, neighboring grid islands are reconnected to restore the larger grid. People who can be part of a grid island that has protected generators or microgrids can work together to survive.

Special attention is needed for protecting power to ensure nuclear power plant cooling systems continue to operate to avoid Fukushima-type disasters. There is a premium on backup diesel generators and sufficient fuel to operate critical equipment necessary for grid restoration. Stocking and pre-positioning of spare equipment, especially hard-to-replace extra high-voltage transformers.

Some issues worth noting regarding a national blackstart capabilities include:

a. It is important to have a clear chain of command in place, agreed on at all levels beforehand among utility company principals and public officials.

b. Without power, there will be public disorder that will require special protection for restoration teams. There will likely be a need for National Guard assistance to law enforcement and force protection provisions. Substations may be used as command post locations to coordinate restoration team activity and provide protection. National Guard communication systems may be helpful to restoration teams in executing their step-by-step recovery process.

c. Unlike generation station recovery, blackstart of the transmission grid will require wide-area communications because coordination with remote locations is necessary. Communications assets used for this purpose under normal conditions include cell phones, dedicated microwave systems, and satellite systems. Following an EMP attack, it is likely that only land-mobile radios and possibly UHF SATCOM may be available. These limitations should be included in plans and exercises.

d. As electronic controls and other critical components of the electrical transmission and generation system suffer damage, so do similar components on the production, processing, and delivery systems providing fuel to the electric generators. Restoration of the electrical power system is not feasible on a wide scale without a parallel restoration of these fuel processing and delivery systems. Many utilities are now switching their primary blackstart facilities from hydroelectric to natural gas plants. This trend is counterproductive from a national resilience standpoint because natural gas pipelines supplying fuel for gas turbine generators may shut down quickly at the outset of triple-threat contingencies. Hydro-plants, coal plants, geothermal, and nuclear plants have longer duration latent fuel supplies, which can expedite the blackstart process and thus avert long-term outages. Beyond hydroelectric and geothermal, coal plants

typically have significant on-site stockpiles of fuel so the delay in rail and other delivery systems for even a month would not be issue for coal-fired plants.

e. At present, NRC rules require nuclear plants to be shut down under blackout conditions. This requirement should be re-evaluated given the multi-year energy output capacity (without reload) of nuclear fuel. Nuclear power plants serve as a strong base power source for avoiding blackouts or restarting other portions of the grid should a blackout occur. Re-engineering of these plants to enable them to operate through or rapidly restart would add significantly to blackstart resources and avoiding Fukushima-type catastrophes. The Nuclear Regulatory Commission has an opportunity to develop a demonstration program to authorize back fitting and augmentation of existing nuclear power plants, associated blackstart generating facilities and "cranking paths" to ensure reliable blackstart re-operation of nuclear generating facilities. To meet safety requirements, applicants should be required to demonstrate the availability of reliable on-site and off-site backup electric power to ensure safe shutdown, protection of spent fuel pools, and reliable operation of control and security systems. Appropriate criteria for cost recovery may involve both the Nuclear Regulatory Commission and the Federal Energy Regulatory Commission (which authorizes blackstart cost recovery), and state public utility commissions.

f. It may take considerable time to restore the grid following a wide-area blackout. Balancing generation and load and then reconnecting each new grid increment are a reasonably difficult and time consuming process in the best of circumstances. A "new normal" interim situation should be anticipated with local grid islands as the main electric power supply for some months. Power will be available within geographic pockets and the electric supply will not operate 24/7 in many of these locations.

5. A single accountable national authority given overall responsibility for EPG resiliency vis-à-vis catastrophic triple threat contingencies.

The FERC-NERC consortium is not set up administratively or legally for national security problem resolution. A national electric power protection executive is needed, with the authority and necessary resources to manage grid resiliency assurance efforts. The executive should be accountable at the NSC/NHSC level.

The executive should be vested with the authority to establish and enforce uniform national electric grid assessment and protection guidelines. Useful standards already exist for EMP, cyber and physical protection. EMP protection standards and guidelines were issued by the DoD in the early 1990s and by DHS in 2016.

Notably, DoD has established a comprehensive set of survivability benchmarks for Defense Critical Infrastructure Protection (DCIP) that could be expanded for use in assessing and protecting critical national infrastructure. These standards and benchmarks were established by the Joint Staff, under their DoD Directive 3020.40 to assist DoD Components and Sector Lead

Agents identify and correct vulnerabilities of their critical assets and supporting foundational infrastructure.

6. Capital investments and cost recovery decisions reviewable and approvable by FERC for the bulk electric system and by state regulators for the distribution system.

The North American electric grid will benefit from both guidelines and mandatory standards that reduce opportunities to attack the electric grid and critical infrastructures at their weakest points. Protection costs for new energy facilities and new communication systems are usually substantially less expensive than retrofit costs. Hence a vision for a more robust electric grid must assure that many standards applicable to the bulk power system are also applicable to interstate energy pipeline systems and within states that license new generating and transmission facilities, through some combination of uniform state laws and limited federal preemption of state standards.

Summary.

It is hoped that this vision for the future will help focus efforts to achieve a grid that is able to withstand or quickly recover from catastrophic failure due to EMP, cyber and physical attacks. The vision rests on the considerable common ground between industry objectives and national security objectives to prevent long-term national-scale outages. Keys to success include strong public-private partnerships, a multi-threat approach based on identifying and protecting single-point vulnerability locations, improved empirically-verified grid effects and recovery models, and oversight by a single accountable national authority with overall responsibility for EPG resiliency vis-à-vis catastrophic triple-threat contingencies. Public awareness is growing and several public-private protection initiatives within several states are paving the way by providing leading-edge examples for the nation to pursue achievable, cost-effective grid resiliency solutions.