

Testimony of Dr. George H. Baker
Professor Emeritus, James Madison University
Director, Foundation for Resilient Societies

United States of America
Before the
Senate Committee on Homeland Security and Governmental Affairs
February 27, 2019

Many thanks to Senator Johnson and Senator Peters for this opportunity to share my thoughts on the protection of our critical national infrastructure against the wide-area electromagnetic threats posed by the nuclear electromagnetic pulse (EMP) and solar storm geomagnetic disturbances (GMD). Protection is urgently needed to assure 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 and test Department of Defense (DoD) systems against EMP. I also directed the Springfield Research Facility, DTRA's assessment arm, responsible for vulnerability assessments of critical military facilities and supporting infrastructure and organizing and deploying the initial Joint Chiefs of Staff (JCS) Force Protection vulnerability assessment teams. In my second career as an academic, I directed James Madison University's Institute for Infrastructure and Information Assurance, developed courses on complex infrastructure systems and how they fail and nuclear energy technology, and organized five national symposia on Critical Infrastructure Assurance in conjunction with the National Research Council. During 2001-2008, and again in 2017-2018, I served as a Senior Advisor to the Congressionally-mandated Commission to Assess the Threat to the United States of Electromagnetic Pulse (EMP) Attack.

The nature of EMP and GMD effects on our grid can be severe, to be sure. These phenomena introduce abnormal transient electrical currents into systems precipitating upset and thermal damage within electrical and electronic components. Consequences involve 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, effective, and practical engineering solutions are available to counter these threats. We have the engineering know-how and tools to protect ourselves. What is lacking is resolve.

I will use today's Senate Roundtable to address questions posed by Senator Johnson and his staff regarding the severity of EMP and GMD system/network effects and the status of national preparedness to operate through and recover from these effects.

Question 1: What are your thoughts on how an EMP/GMD would impact the electric power grid?

Atmospheric nuclear tests and simulated threat-level EMP testing reveals that systems connected to long lines are especially vulnerable to component damage, necessitating repair or replacement. All three time phases of the EMP waveform (E1, E2, and E3) couple most efficiently to long lines, and would induce thousands of amperes on each overhead line that you see as you drive down major highways. Because the strength of EMP fields is measured in volts per meter, to first order, the longer the line, the more EMP energy will be coupled into connected systems and the higher the probability of system damage. Furthermore, the levels of EMP current and voltage induced on lines increase with lines' height above ground. Because of its organic, elevated long lines, the electrical power grid is, itself, highly vulnerable to component damage when exposed to EMP and will couple large electrical transients to most other (dependent) infrastructure systems. It is ironic that our most critical infrastructure is also the most

vulnerable to EMP, i.e. the grid couples the highest EMP/GMD levels into its own components and those of connected facilities and systems.

The U.S. 1962 Starfish Prime high altitude burst nuclear test 900 miles from Hawaii provided partial evidence of EMP's capabilities. The absence of large-scale infrastructure failure in Honolulu is the favorite anecdote of EMP skeptics, used over and over as evidence that we need not worry about long-term grid collapse from EMP. However, the Hawaiian Islands were in the far-field, low-amplitude fringe of the EMP geo-pattern, the burst height and weapon design were non-optimal for EMP field generation, and the electronics technology common in today's electric power, communication, Internet and control systems was absent from the Hawaiian networks. The small geographic size of the islands and corresponding short lengths of power lines, greatly reduced E3 effects on the grid. Thus, the Starfish Prime test offered a highly limited ensemble of possible EMP effects – just a small taste of things to come.

Because their high-altitude nuclear bursts were over a continental landmass, exposing long line networks spanning thousands of miles, the Russian atmospheric nuclear test experience has provided many more insights into EMP effects. But, just as with U.S. tests, the Russian test lessons are limited by the absence of today's electric power, communication, Internet and control systems. The Russian tests caused overhead transmission and telecommunications line disconnects and damage including electrical arc breakage of powerline support insulators, causing overhead power lines to drop to ground. Dr. Valery Kondrat'ev reported they experienced fires from EMP and loss of communications gear. Military generators (fixed diesel generation plants) and substations were damaged. Overhead line network damage was due to early-time EMP and buried cable damage by late-arriving EMP. The Russians also reported malfunctions of radio stations.¹

Since the atmospheric test era, government and industry laboratory tests of hundreds of items have revealed EMP vulnerability of grid distribution transformers, grid control electronics, computers, and communication networks and indicate that we have become more vulnerable to EMP due to technology advances and the foundational role of electricity and electronics in our everyday life and enterprise-enabling infrastructures.

Without protection, there is real evidence from atmospheric testing and laboratory testing that the grid will collapse, causing long-term, large-scale cascading debilitation of dependent infrastructures and services. EMP system debilitation is due to the upset and thermal burnout of grid-essential command, control, and communication electronics, and physical damage to the heavy-duty grid components that supply our power including transformers, and possibly generators. The military has the benefit of decades of system testing and a classified database documenting EMP effects on hundreds of systems that has caused them to recognize that the electric power grid, in its present unprotected state, cannot be relied on following an EMP attack. The military includes hardened backup power as part of mission essential system design. DoD is installing hardened "microgrids" on key bases to make them independent of the surrounding grid.

Because the power grid is essential to the recovery of all critical infrastructure sectors, the ability to operate through an attack or to be rapidly restored is paramount. For example, emergency responder experience during multiple severe hurricanes indicates that electric power availability is critical for their operations.

¹ H. Seguire, U.S.-Russian meeting – HEMP Effects on National Power Grid and Telecommunications, National Communication System Memorandum for Record, 17 Feb. 1995

I'm sure you'll hear from other witnesses that "EMP effects are not that bad – not to worry" and "it's not necessary to harden the grid, rather let's put our money into recovery phase activities, spare parts, etc. so we can pick up the pieces afterwards." Threat levels, as defined by many utilities and their research arms, is based on optimistic assessments using EMP/GMD waveforms that are lower than levels predicted by the latest empirically-verified science and, in the case of GMD, lower than measured solar storm levels.

The utility industry's "minimization mindset" is dangerous. As a case in point, the Federal Energy Regulatory Commission (FERC)/North American Electric Reliability Corporation (NERC) GMD standard (TPL-007-2) which set GMD Earth potential levels lower than those measured during past solar storms and set transformer failure thresholds higher than known malfunction levels. The result of this rosy industry analysis was that only fourteen of the thousands of transformers included in the model, would need protection – a result far from consensus among independent experts. Even with enforced utility compliance with the present GMD standard, our grid will remain vulnerable to major solar storms.²

Government officials and utility executives must transition to a "defense-conservative" mindset for our power grid and other lifeline infrastructures – just as our military does in protecting our strategic systems.

Question 2: How is the private sector evaluating and attempting to address the threat of an EMP/GMD?

The FERC GMD standard (TPL-007-2), though its specified environments and system thresholds are not defense-conservative, has at least brought industry attention to GMD effects. Because there is no corresponding federal EMP directive, the private sector is not doing very much of anything to address the EMP threat. The absence of federal EMP directives and standards for the electric power grid has resulted in inconsistent industry interest, approaches and questionable protection effectiveness.³ The NERC/electric industry EMP approach appears to be to let the national grid fail and concentrate attention, investments and preparedness on elaborate recovery plans to rebuild the grid in the aftermath of an EMP-caused grid collapse. This approach is fraught with risk.

There have been a few glimmers of EMP interest and action including several uncoordinated efforts within the electric power industry and IT/Communication/Data Center industry. Center Point, PJM, and Dominion Energy have each hardened a major control center. AEP has protected 400+ substation control shelters. Generation stations have not been addressed because of cost-recovery limitations (unlike transmission systems where federal regulations allow cost recovery). Notwithstanding, other than a beta-test of a GMD protection device for one transformer in Wisconsin, no hardening of the bulk power system's high voltage, heavy duty, long-lead-time replacement items has occurred. The grid, in its current unhardened state, would likely be out of service for long periods following a major solar storm or EMP attack.

Within the communications/Internet sector, one major data center in Indiana, belonging to an insurance company, has been protected. A data center in Minneapolis that serves electric utility industry has installed a small protected space. One data center in Pennsylvania has EMP-protected a space of about 2000 square feet. Companies are reluctant to harden because there are no EMP/GMD regulations or requirements for civilian infrastructure. Power industry officials have expressed reservations that any

² Electric Power Research Institute, Magnetohydrodynamic Electromagnetic Pulse Assessment of the Continental U.S. Electric Grid. Palo Alto, CA, February 2017.

³ W. R. Graham et al, Assessing the Threat from Electromagnetic Pulse (EMP), Executive Report, Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, July 2017

near-term protection initiatives could well be rendered obsolete if they don't conform to unknown future regulations and standards.

A major national concern is that a significant number of local electric power microgrids are being installed around the U.S. with no EMP protection. Microgrids are being justified and installed at highly-critical infrastructure sites that cannot tolerate even short-term electric power grid outages. Thus, failure in an EMP event would likely terminate essential microgrid-powered services. Another major concern is that installation of unprotected microgrids actually harms the resilience of the existing grid by increasing the “vulnerability of complexity.”⁴

Microgrids add another layer of complexity to the existing grid. Grid EMP vulnerability is increased by the additional coupling pathways inherent in microgrid control electronics networks and interconnecting powerline pathways. Federal requirements would be very helpful to ensure microgrids will survive and not increase the EMP vulnerability of the rest of the grid. Note that microgrid EMP protection introduces a small incremental cost if included in initial system design, adding only 2-5% to microgrid acquisition costs. Based on DoD experience, retrofit EMP protection costs run ten times higher. We are at a watershed moment where we must decide between designed-in protection on microgrid installations yielding much improved electricity supply resilience – or proceed in our current lazy-faire manner with resulting increases in local and regional electric power grid vulnerability.

Regrettably, industry and government are largely ignoring the Congressional EMP Commission's findings and recommendations. Recent National Infrastructure Advisory Council (NIAC) and Congressional Research Service (CRS) reports have also ignored recommendations from knowledgeable public interest groups, including the Foundation for Resilient Societies^{5,6,7}, JINSA⁸, The American Foreign Policy Council⁹, Infragard's EMP Special Interest Group¹⁰ and the US Air Force Training Command's Electromagnetic Defense Task Force (EDTF)¹¹. A survey of recent government reports that address the protection of critical infrastructure reveals that none mention EMP, although critical infrastructure risks, resilience, protection, and availability are central to each report and to each Departments' mission¹². Key reports on infrastructure protection and nuclear posture neglect to address

⁴ The “vulnerability of complexity” was coined by Yale professor Charles Perrow in his book, Normal Accidents. “Normal accidents” in complex infrastructure systems involve system interactions that are not only unexpected, but are incomprehensible for some critical period of time. For instance, it took an expert NERC investigation team three months to determine the exact combination and sequence of system failures that led to the 2003 Northeast blackout.

⁵ G. Baker, W. Harris, T. Popik, Protecting the Electric Power Grid from Electromagnetic Pulse: Legal and Policy Aspects, Critical Infrastructure Protection Report, George Mason University, July 2013.

⁶ T. Popik, W. Harris, G. Baker, Comments of the Foundation for Resilient Societies on The Federal Energy Regulatory Commission Reliability Standard for Transmission System Planned Performance for Geomagnetic Disturbance Events, Docket No. RM15-11-000, 10 August 2015.

⁷ T. Popik, Testimony of the Foundation for Resilient Societies before the Federal Energy Regulatory Commission Reliability Technical Conference, Docket No. AD16-15-000, 1 June 2016

⁸ B. Gabbard, R. Joseph, Threats to U.S. Critical Infrastructure, Gemunder Center EMP Task Force, September 2015

⁹ R. Harrison, I. Berman, Strategic Primer: Electromagnetic Threats, American Foreign Policy Council, Winter 2018.

¹⁰ M. Laskey, W. Harris, S. Volandt, Powering Through: From Fragile Infrastructures to Community Resilience, Infragard EMP Special Interest Group, November 2016.

¹¹ D. Stuckenberg, R. Woolsey, D DeMaio, Electromagnetic Defense Task Force (EDTF) 2018 Report, Air University Press, Maxwell Air Force Base, Alabama, November 2018.

¹² These reports include Mitigation of Power Outage Risks for Department of Defense Facilities and Activities 2015, National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and

EMP. EMP is not included in the DHS list of top 100 threats. EMP programs will greatly benefit from attention to reports from all concerned organizations and must have more attention at the highest policy levels.

On a positive note, several commercial enterprises have developed turn-key EMP services and product lines and stand ready to harden critical infrastructure facilities and systems (see Figure 1). I am confident that, once we have national, state and local protection initiatives, American companies will be ready to harden critical infrastructure facilities and systems. Because U.S. firms are world leaders in EMP protection technologies, there is good potential for well-paying manufacturing and installation jobs in this emerging industry. Our allies also need EMP protection, so there is the opportunity for robust export of EMP protection devices and services.

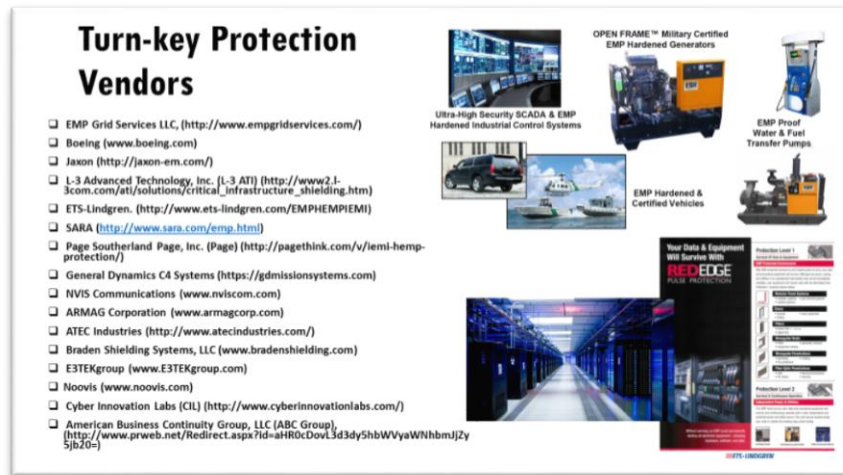


Figure 1. Turn-Key EMP/GMD Protection Vendors.

Question 3: What is the potential cost of hardening our nation’s electrical grid with respect to available technical options?

There have been several efforts to quantify the cost to harden the grid. None have been conclusive. An early effort by the Foundation for Resilient societies estimated costs in the several tens of billions of dollars for the bulk power system and supporting communication, fuel and transportation infrastructures (Figure 2). Note that generation stations, not subject to FERC protection standards, likely represent the largest share of EMP/GMD protection costs.¹³

Resilience (DHS), U.S. Department of Energy Strategic Plan 2014-2018, and the 2018 Nuclear Posture Review.

¹³ Note: DTRA has recently (Fall 2018) begun the first HV generation station EMP testing.

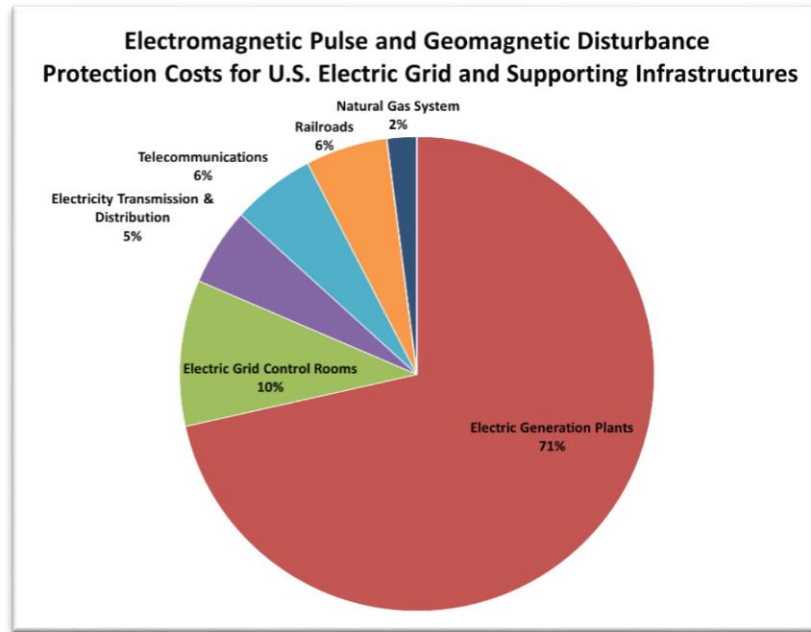


Figure 2. Protection Costs Breakout for Electric Power Grid and Supporting Infrastructures, Foundation for Resilient Societies.

Based on the work of the Foundation for Resilient Societies and DoD experience in hardening military systems, my preliminary estimate for prioritized protection of the existing electric power system is on the order of \$50B, representing about 1% of the grid’s replacement cost. From a cost-benefit standpoint, this amount is reasonable when compared with the dollar losses from a national-scale blackout which would be measured in multiples of the U.S. GNP (tens of trillions of dollars). The estimate considers protection of a top-down “thin-line” of priority grid systems including selected HV generation plants with priority given to nuclear plants and black-start plants, selected transmission substations (e.g., FERC’s analytical result of nine critical substations in the U.S. electric grid), plus the control centers and communication networks necessary for monitoring grid status and controlling post-event restoration efforts. Some of the necessary fuel logistical tail (transportation assets, pipelines, transfer terminals, refineries) is also included in this rough estimate. This level of investment would allow faster reconstitution of the bulk grid following an EMP or GMD-caused grid collapse but would not offer complete protection. The investment strategy is based on identifying a top-down “thin-line” of grid assets necessary to restart the bulk power grid. For a more rigorous and complete cost estimate I recommend cost studies by DOE, industry, and independent think tanks.

A bottom-up EMP protection approach (local, State efforts) and cost estimate is also required since communities could be on their own for extended periods in a wide-area blackout. Local community awareness is essential to develop effective programs that address a thin-line of life-support infrastructures including local backup power generation systems, emergency services (law enforcement, fire, EMS, and their communications), water supply/treatment, hospitals, and the necessary logistics tail (food, fuel). The Carolinas’ Lake Wylie project provides a model for costing a bottom-up EMP/GMD protection program. The federal government needs to coordinate the interface between the top-down and bottom-up efforts. The interface demark occurs where the high voltage transmission grid (bulk power) meets the distribution grid (lower voltage electric network supplying local infrastructure services).

Low cost stop-gap measures will be important, including hardened microgrid installations as a near-term solution for life-line infrastructures. As mentioned, we are presently at a watershed moment due to the

onset and rapid acceleration of microgrid installations. Federal EMP standards are desperately needed to inform and govern the protection of microgrids. Otherwise, microgrids will actually increase the vulnerability of the existing grid due to the added layer of complexity, including heavy reliance on microprocessor controls vulnerable to the E1 pulse. While I commonly learn about efforts to protect commercial systems against EMP, I would be hard-pressed to give a good example of EMP-protected microgrids in the civilian infrastructure. Accordingly, I estimate that the microgrids now being developed and installed would fail under EMP attack conditions.

Question 4: What additional authorities would you recommend and should be involved to assure national preparedness to withstand an EMP/GMD event?

To sharpen our resolve and policy objectives for EMP/GMD preparedness, federal authorities must recognize that America's grid is the prime target infrastructure of our adversaries. Because the electric power grid is the foundation of our technical society, in military parlance, an EMP attack engenders the ultimate "functional defeat" of the American society and enterprise. Debilitation of the electric power grid would lead to an internecine fight for survival. Without protection and planning, our society would internally self-destruct, greatly diminishing an attacker's required follow-on war effort to take over America's land possessions, island territories such as Guam, the remote states of Hawaii and Alaska, and even the continental United States.

The single most important recommendation of the 2018 EMP Commission Executive Report was to establish an office of EMP coordination within the National Security Council (NSC).¹⁴ The Commission recommended immediate action to advance U.S. security and survivability with the President establishing an Executive Agent having the authority, accountability, and resources to manage U.S. national infrastructure protection and defense against EMP. The Commission expressed concern that the current institutional authorities and responsibilities – government, industry, regulatory agencies – are fragmented, incomplete, under-resourced, and unable to protect and defend against foreign EMP threats or major solar storms.

The new EMP executive order, if signed, will help in this regard by designating the Assistant to the President for National Security Affairs (APNSA), through the NSC and in consultation with the Director of the Office of Science and Technology Policy (OSTP), as responsible for coordinating the development, and implementation of executive branch activities related to national EMP preparedness.

Certain aspects of the Energy Power Act of 2005 have become detrimental to national preparedness against EMP attack. The self-regulatory system for electric utilities, with NERC as the designated Electric Reliability Organization (ERO) has, in effect, neutered FERC. Under the Act, FERC can request standards but cannot write them. In the quest for national EMP/GMD preparedness, FERC serves only as the brake pedal rather than the driver. Through a sua sponte order to NERC, FERC requested only a GMD standard, intentionally excluding EMP protection. The resulting NERC GMD standards (TPL-007-1 and TPL-007-2) enable utilities to sidestep grid protection engineering using paper studies. The few items of long-replacement-time grid equipment that would be protected to NERC's sub-threat TPL-007-1/2 solar storm standards would remain vulnerable to substantially higher magnitude HEMP E1 and E3 hazards, with risk of E1 damage to circuits and relays required to protect against E3. A combined-threat EMP-GMD standard is a needed and cost-effective solution.

¹⁴ W. R. Graham et al, Assessing the Threat from Electromagnetic Pulse (EMP), Executive Report, Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, July 2017

New legislation is needed to empower FERC, specifically to enable the Commission to write and enforce grid protection standards.¹⁵ We must give FERC authority commensurate with Nuclear Regulatory Commission's reactor authority, but over the US power grid. FERC should have explicit authority related to improving national security. FERC should also be asked to identify regulatory and non-regulatory mechanisms, including cost recovery measures, to incentivize private sector engagement to address the effects of EMP. In legislation, FERC should also be asked to develop a national-level blackstart plan. Currently we have only local and regional black start plans where utilities assume they can blackstart themselves by tapping into nearby, unaffected grids – an untenable approach in a continental-scale EMP/GMD contingency.¹⁶

NERC's role should also be redefined to coordinating and assuring industry compliance with FERC EMP/GMD standards. FERC and NERC should report to NSC and Congress on a regular basis on the status of the overall resilience, security, and protection state of the U.S. electric power grid.

A persistent barrier to the approval and implementation of effective grid reliability standards has been inadequate cost recovery opportunities.¹⁷ 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 a countervailing effect on reliability. The adage, "private efficiency leads to public vulnerability," applies here.¹⁸ Better designed electricity markets with incentives reducing multi-hazard risk of catastrophe would lead to major improvements in grid resiliency.

The Director of National Intelligence plays key role by determining foreign aggressors' intent and capabilities regarding EMP. Agencies use DNI briefings and reports in determining whether or not to include EMP in their planning and requirements. Unfortunately, the most recent intelligence community (IC) EMP report published by the Joint Atomic Energy Intelligence Council (JAEIC) is factually erroneous and analytically unsound. This report provides an effective excuse/alibi for agencies and their industry affiliates to ignore EMP in their planning and system acquisition processes. The Congressional EMP Commission recommended that the DNI circulate to all recipients of the 2014 JAEIC report the EMP Commission critique of that report and direct a new assessment that supersedes the 2014 JAEIC EMP report. The new IC report should be reviewed by experts in the subject areas being addressed and circulated to all the recipients of the defective 2014 assessment.

EMP is not mentioned in several important high-level policy documents including the U.S. Department of Defense 2018 Nuclear Posture Review. EMP is not mentioned in the Department of Homeland Security list of top 100 threats. I ask your Committee for the inclusion of the EMP threat at the highest levels of policy guidance, especially when your Committee has oversight responsibility.

¹⁵ The DOE Quadrennial Energy Review released in January 2017 recommended, "... in the area of cybersecurity, Congress should provide FERC with authority to modify NERC-proposed reliability standards—or to promulgate new standards directly..." EMP could be included under the cyber threat since it debilitates cyber electronic systems and constitutes the ultimate denial-of-service attack.

¹⁶ G. Baker, Testimony before the Federal Energy Regulatory Commission Reliability Technical Conference, Docket No. AD17-8-000, 22 June 2017

¹⁷ Ibid.

¹⁸ P. Auerswald et al, Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability, Cambridge University Press, 2006.

Question 5. How can current DHS and DOE programs improve efforts to protect critical national infrastructure against EMP and GMD?

The impending EMP Executive Order will help and goes a long way in clarifying DHS and DOE EMP/GMD roles and responsibilities.

Because we can't protect everything, progress will be spurred by a prioritized list of EMP-susceptible infrastructure from DHS. Developing criteria for prioritization would benefit from coordination with Assistant Secretary of Defense (Homeland Defense and Americas' Security Affairs) on their criteria for assembling the Defense Critical Asset (DCA) and Defense Critical Infrastructure Protection (DCIP) lists. A recovery time objective (RTO) should be specified for critical infrastructures and used as a criterion for priority assignment.

Due to its 50-plus year learning from actual EMP specification, design, build, and test experience, DoD information sharing and assistance to DHS and DOE is crucially important to national preparedness. The U.S. military already has EMP protection approaches that are practical, affordable, 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, DoD has protected high priority military command, control, and computer assets for nuclear deterrence and response. DHS and DOE EMP/GMD protection programs should emulate DoD's efforts.

In this vein, it will be important to preclude temptations to re-invent the wheel by giving DHS and DOE full access to DoD standards, handbooks and data bases. Existing EMP standard waveforms are more than adequate for specifying a standard unclassified EMP environment for use by industry. In particular, the International Electrotechnical Commission's (IEC) E1 and E2 waveforms¹⁹ coupled with the EMP Commission's E3 waveform²⁰ provide an excellent, unclassified basis for national infrastructure EMP protection. These coupled with the MIL-STD-188-125 shielding effectiveness acceptance test and pulsed current injection (PCI) acceptance test specifications will provide high confidence in critical infrastructure system survivability. Systems complying with the MIL-STD-188-125 E3 PCI acceptance test will also survive 100-year solar storm GMD-induced currents.²¹

It will be important for DHS and DOE to develop expertise with DoD EMP protection, testing and hardiness maintenance and surveillance HM/HS programs. EMP/GMD assurance does not end with initial installation of protection hardware. DoD has found that EMP hardiness degrades with time, necessitating periodic system surveillance and maintenance. Critical infrastructure protection (CIP) programs should include outyear funding for this. A paragon hardiness maintenance program is STRATCOM's Minuteman HM/HS activity.

Stove-pipe attention to single threats necessitate needless and unnecessarily expensive redundancies in system protection. DTRA's blue ribbon assessment programs have found that all hazards protections are imminently practical – 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. The failure of current GMD protection efforts to address nearly identical vulnerabilities and protection measures for the EMP/E3 waveform has been a lost opportunity.

¹⁹ International Electrotechnical Commission, EMP Environment Standard 61000-2-9

²⁰ Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. *Recommended E3 HEMP Heave Electric Field Waveform for the Critical Infrastructures*. Report of the EMP Commission, July 2017.

²¹ Note: EMP protection covers GMD effects. Late-time EMP (E3) protection hardware will suffice for GMD protection.

Grid vulnerabilities can be reduced by hardening the electric grid and, procedurally, by executing well-planned load shedding given adequate warning time (EMP can occur with no warning). Smart, timely reconstitution of the grid following a planned or unplanned shut-down is an equally important part 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. This will be key to cost reduction. DOE has included provisions for improved grid modeling in its 2016 EMP Action Plan.

Empirical validation of models is essential for confidence building. Electromagnetic system effects and hardening requirements are tried and true for communication, computer, and control electronics due to DoD protection and test programs and standards development. However, there are still holes in our system testing and hardening data bases. Of most concern, we have not yet tested or hardened HV generation plants and HV/EHV transformers. Threat level testing will be required to determine EMP/GMD vulnerabilities, develop and validate models, and verify protection methods. To this end, new and upgraded EMP/GMD integrated system test beds are needed. The Idaho National Laboratories (INL) and Tennessee Valley Authority (TVA) are excellent candidates for test beds and have begun initial development. And Duke Energy has recently provided a large transformer for the first U.S. HV transformer test.

Pilot demonstration programs in selected grid sectors are all-important to answer questions on feasibility and cost of local and regional infrastructure EMP protection. The cost of grid EMP protection is the biggest question out there. The ongoing Lake Wylie Protection Project and the San Antonio Joint-Base microgrid development programs are good examples and should be encouraged, expanded, and funded.

DHS should publish an official, unclassified EMP/GMD standard. DHS is to be commended for issuing a coordination version of a communication/data center protection standard.²² This document should be expanded to include HV/EHV electric power assets (HV generators and substation transformers/breakers). In addition, a DHS-endorsed national EMP/GMD planning scenario would provide an overarching scope for public and private stakeholder awareness, grid protection and recovery planning. DHS needs to expand its complement of EMP/GMD scientists and engineers.

Summary and Action Items.

To sharpen our resolve and policy objectives for preparedness, Federal authorities must recognize that America's grid is the prime target infrastructure of our adversaries. Despite witness arguments to the contrary, the grid, in its current unhardened state, would likely be out of service for long periods following a major solar storm or EMP attack. Our strategy must be defense conservative and to enable as much of grid to survive as possible. I recommend the following steps to achieve grid resilience, including 'top-down' actions and a set of equally important 'bottom-up' actions.

- From a Top Down perspective:
 - The most important recommendation of the 2018 EMP Commission was to establish an office of EMP coordination within the National Security Council (NSC). The new EMP executive order does this.

²² Electromagnetic Pulse (EMP) Protection and Resilience Guidelines for Critical Infrastructure and Equipment, Version 2.2, DHS National Coordinating Center for Communications (NCC), National Cybersecurity and Communications Integration Center, February 2019,

- The FERC GMD standard (TPL-007-2), though its specified environments and system thresholds are not defense-conservative, has at least brought industry attention to GMD effects. This standard, even if rigorously enforced will leave the grid dangerously vulnerable to GMD. The standard must be revised.
- Without a corresponding FERC EMP directive, the private sector is not doing very much of anything to address the EMP threat. An EMP directive and environment standard are sorely needed.
- New legislation is needed to empower FERC, specifically to
 - (1) Enable FERC to write and enforce grid protection standards.
 - (2) Identify mechanisms, including cost recovery measures, to incentivize private sector engagement on EMP protection and increase on-site fuel stockpiles.
 - (3) Develop a national blackstart plan.
- A national EMP protection standard is needed. DHS is to be commended for issuing a coordination version of a communication/data center protection guidelines. DHS should expand this to include HV electric generator stations and electric substations.
- For more than a half-century, DoD has protected high priority military command, control, communication, and computer assets for nuclear deterrence and response. DHS and DOE EMP/GMD protection programs should emulate DoD's efforts.
- We must preclude the temptation to re-invent the wheel by giving DHS and DOE full access to DoD standards and data bases. There is no need to recalculate a standard EMP waveform. Note that current EPRI grid vulnerability assessment models are using low-bound recalculated E3 waveforms. Existing IEC and EMPC EMP waveforms are more than adequate. Use of the unclassified MIL-STD-188-125 test regimen will assure power grid survivability to both EMP and 100-year solar storms.
- A prioritized list of EMP-susceptible infrastructure is needed. System protection and reconstitution prioritization requires improved grid modeling. Integrated system test beds will be important for model validation. Top priority is HV generation plants and HV/EHV transformers, heretofore untested. The INL and TVA test beds look promising.
- The most current EMP Intelligence report is technically flawed and misleading in a manner that downplays the need for action – a new assessment is needed.
- I estimate cost of EMP protection for the bulk power system to be in the \$50B range. The investment strategy is based on identifying a top-down “thin-line” of grid assets. More rigorous cost estimates are needed by DOE & industry.
- From a Bottom-Up perspective:
 - EMP protection programs must be pursued at the local and State levels since communities would be on their own for extended periods in a wide-area blackout.
 - Pilot demonstration programs of selected grid sectors are all-important to address the feasibility and cost of local EMP protection. The ongoing Lake Wylie Demonstration Project and the San Antonio Joint-Base microgrid development program are good examples and should be expanded and funded.
 - Bottom-up protection should address a thin-line of essential life-support infrastructures including distribution substations, backup power generation systems, emergency services, water supply and treatment, hospitals, and the necessary logistics tail.
 - Low cost, stop-gap measures will be important, including hardened microgrid installations as a near-term solution for life-line infrastructures. We are presently at a watershed moment due to the recent onset and rapid acceleration of microgrid installations. Federal requirements and standards are important to ensure that microgrids will survive and not increase the EMP vulnerability of the rest of the grid. Microgrid EMP protection is only a small incremental cost if included in initial system design.

Testimony of Dr. George H. Baker before the Senate Homeland Security Committee

- The federal government must coordinate the interface between the top-down and bottom-up efforts. A useful interface demark occurs where the high voltage transmission grid (bulk power) meets the distribution grid (lower voltage electric network supplying local infrastructure services).
- On a positive note, several commercial enterprises have developed turn-key EMP protection services and product lines and stand ready to harden critical infrastructure facilities and systems once directives and programs are in place.