Electromagnetic Pulse Resilience of United States Critical Infrastructure: Progress and Prognostics

George H. Baker[1]

[1]Professor Emeritus, James Madison University, bakergh@jmu.edu

Thanks largely to Presidential Executive Order 13865,[1] national electromagnetic security vis-à-vis the nuclear electromagnetic pulse (EMP[2]) and solar geomagnetic disturbances (GMD) has received substantial attention at the highest levels of the U.S. national policy and technical establishments. Despite diversion of national security efforts to Covid-19 pandemic response, there is notable progress on the electromagnetic security front since the executive order's debut in March 2019. Executive order activities have provided important insights into priority system identification, interdependency, EMP susceptibility, protection requirements, hardening methods (including some new technologies), and protection costs. EMP environment benchmarks for critical national infrastructure have been established and published.[3] NOAA and USGS are continuing efforts to map U.S. and Canadian geoelectric properties and developed improved models of electric power EMP/GMD response. A pilot demonstration program at Joint Base San Antonio has been especially helpful by successfully establishing federal/state/local/industry public-private partnerships for the expressed purpose of implementing EMP resilience including electric power, communication/control systems, emergency services, fuel supply, and water supply infrastructures. The executive order has invigorated Department of Defense (DOD), Department of Homeland Security (DHS), and Department of Energy (DOE) efforts and cooperation in addressing the significant challenges associated with national EMP preparedness. It is important to note that EO 13865 requirements are also mirrored in the FY2020 National Defense Authorization Act (NDAA) passed by the Senate in December 2019.[4]

This paper primarily focuses on civilian infrastructure preparedness. DOD's past and ongoing success in assessing, prioritizing, and protecting military systems from EMP threats has paved the way for the civilian critical infrastructure resilience programs spurred by the Executive Order. The military has a 50-year head start on the civilian sector in achieving EMP resilience.

---

1 Coordinating National Resilience to Electromagnetic Pulses, Executive Order 13865, Presidential Documents, Federal Register Vol. 94, No. 61, p. 12041-12046, 29 March 2019.

2 The EMP acronym as used here refers to EMP produced by a high-altitude nuclear burst.

3 D. Brouillette, Physical Characteristics of HEMP Waveform Benchmarks for Use in Assessing Susceptibilities of the Power Grid, Electrical Infrastructures, and Other Critical Infrastructure to HEMP Insults, U.S. Secretary of Energy Memorandum, January 2021

4 https://www.hsgac.senate.gov/media/majority-media/sen-johnson-statement-on-bipartisan-hsgac-emp-gmd-legislation-in-ndaa

doi: 10.18278/jcip.2.1.5

The large geographic areas exposed by EMP and GMD events, the ubiquity of systems affected, and hardening costs, require careful discretion in downselecting the systems and facilities to protect. Priority system identification requires locating critical life-support services (e.g., electric power, water plants, fuel supply, communications network operation centers, transportation hubs) and national security facilities (strategic bases, war headquarters, national essential function (NEF) sites, etc.). Risk assessment based on combined function and fault tree analysis of life and security critical services will be important to identify priority infrastructure systems. Assigning a "recovery time objective (RTO)" in hours, days, or weeks will help in ranking systems to protect. Some systems must be able to "operate through" an EMP/GMD contingency, while others have lower time urgency and can be allowed to fail if provision is made for repairing the systems and restoring their electric power and communication/control connectivity within their specified RTO.

DHS leads the priority system identification process and has initially placed the electric power and communications sectors at the top of their list vis-à-vis EMP protection. These infrastructures exhibit the highest electromagnetic susceptibility due to the large EMP/GMD coupling cross-sections of their long mission-essential connecting lines. DHS is expanding their priority list by identifying the additional infrastructures supporting the operation of electric power and communications.

Thanks to DOD's attention to EMP effects and hardening since the 1960s, including the development of handbooks and standards, protection engineering solutions are known, tried, and true.[5] DOD's success in producing peer-reviewed techniques and guidelines have enabled us to begin protecting priority infrastructure without delay. Electromagnetically simple systems with a contiguous shield and a limited number of protected penetrations will survive EMP. The governing engineering principles are straightforward. These include minimizing the volume of the space occupied by mission-critical electronics, enclosing this equipment in a single continuous shield (use of multiple shielding layers significantly complicates the hardness surveillance and maintenance processes), limiting the number of electromagnetic penetrations through the shield, and protecting all remaining penetrations. The engineering approach also includes certifying the hardness of protected systems via shielding effectiveness measurements and current injection tests of cable penetrations, plus periodically retesting system shielding and penetration protection to ensure continuing hardness integrity. Numerous systems, both military and civilian, have successfully implemented the military standard approach in an affordable manner. EMP mitigation measures are becoming part of the industrial and public consumer culture. Thanks in large measure to DOD,

5 G. Baker, Evolution and Rationale for United States Department of Defense Electromagnetic Pulse Protection Standard, *Insight Magazine*, Vol. 19, Issue 4, December 2016.

EMP protection hardware is now readily available as well as protection installation and testing by turn-key full system EMP protection contractors for communications and data processing systems and facilities as well as emergency backup power systems.

As noted, DHS has initially designated electric power and communications as the top priority infrastructure categories. These infrastructures are not only the glue supporting and interconnecting all other infrastructures during normal situations, but they must also operate early in crisis situations to provide situational awareness and to enable emergency responder efforts to restore other infrastructures. The President's National Security Telecommunications Advisory Council (NSTAC) has also identified these two infrastructures[6] as essential in preventing long term national disasters.[7] It is essential to also identify, include, and protect other infrastructures in our priority list that are necessary for the operation of power and communications. Down-selection of the power and communication sites to harden must take into account national security and lifeline infrastructures in all sectors to ensure that their energy and communication requirements are met.

Electric Power Grid Resilience

The electric power grid and its supporting infrastructures are at the forefront of present national "electromagnetic security" efforts. The electric power grid is arguably the most critical infrastructure, but lamentably it is also the infrastructure most vulnerable to EMP/GMD.[8] Achieving EMP/GMD resilience of the national grid must incorporate both a top-down effort to protect our bulk electric generation and transmission system, and a bottom-up effort to protect electric distribution system and electric power CI customers.[9]

The top-down approach focuses on protecting the bulk-power electric system (BES). In order to ensure the situational awareness that is necessary to avert and respond to outages, system operators' central control facilities and communication-data networks must be the top priority. Protection of the power generation and transmission elements of the BES begins with blackstart and nuclear generation stations. Blackstart and islanding processes must be developed and exercised

6 Report to the President on Telecommunications and Electric Power Interdependencies: The Implications of Long-Term Outages, National Security Telecommunications Advisory Council, December 2006.

7 NSTAC identified the phenomenon of a "Long-Term Outage" (LTO), which it defined as "an interruption of communications and/or electricity for a period long enough, and within a large enough geographic region, to hamper providing communications and electric power by even alternative means." LTOs are also commonly referred to as "black sky events."

8 G. Baker, "EMP Knots Untied: Some Common Misconceptions about Nuclear EMP," Proceedings, Dupont Summit, Carnegie Institute, Washington, D.C., 2013.

9 G. Baker, Written Testimony before the Senate Committee on Homeland Security and Governmental Affairs, February 27, 2019.

over regions up to and including CONUS-wide. A previous Federal Energy Regulatory Commission (FERC) effort to identify and prioritize U.S. electric power facilities will significantly reduce the costs to protect the BES.

The bottom-up EMP protection approach involves protecting the distribution grid and life-supporting services, under the jurisdiction of State and local governments. Since communities are likely to be on their own for extended periods in a wide-area blackout, local community awareness is essential. EMP preparedness programs should identify and address a thin line of life-support infrastructures including local backup power generation systems, emergency services (law enforcement, fire, EMS, and their communication systems), water supply/treatment, hospitals, and the necessary logistics tail (food, fuel, and transportation). The San Antonio Electromagnetic Defense Initiative and the Carolinas' Lake Wylie project provide models for completing a bottom-up EMP/GMD assessment and protection program for a minimum set of essential systems.

The federal government will play an important role in coordinating the interface between the top-down and bottom-up electric power protection efforts. The interface demark occurs at substations where the bulk power high voltage transmission grid meets the lower voltage (< ~100 KV) distribution grid supplying local public and industry user services.[10] FERC has jurisdiction over the higher voltage BES, while States have jurisdiction over the lower voltage distribution systems.

To protect the higher voltage systems that generate, transmit, and distribute electricity, overvoltage protection and low pass filtering techniques have been applied successfully to limit the fast EMP pulse (E1).[11] Solutions for the slow EMP/E3 and solar GMD pulses have been developed and partially demonstrated. Neutral blocking devices offer promise,[12] but require further beta testing at additional grid locations, especially generator step-up transformers (GSUs). We know that large transformers are susceptible to damage from quasi-DC GMD and EMP-E3 surges. There is limited evidence that BES generators are also susceptible to damage.[13] Proposed E3/GMD grid system fail-safe disconnection and islanding solutions also need to be tested on larger scales. The EMP (E1, E2, and E3/GMD) threat-level laboratory test data base for large transformers and BES generators is lacking such that prevalent assertions concerning vulnerability or invulnerability cannot be substantiated at present. It is encouraging that the Idaho National Laboratory and Savannah River National Laboratory have developed detailed propos-

10 G. Baker, Senate Testimony, op. cit.

11 For a brief tutorial on E1 and E3 see https://works.bepress.com/george_h_baker/32/

12 F. Faxvog, G. Fuchs, W. Jensen, D. Wojtczak, M. Marz, S. Dahman, "HV Power Transformer Neutral Blocking Device Operating Experience in Wisconsin," MIPSYNCON, November 2017.

13 L. Marti, A. Rezaei-Zare, Generator Thermal Stress during a Geomagnetic Disturbance, IEEE 978-1-4799-1303-9/13, Toronto, Canada, 2013.

als to develop the necessary test beds. The Interagency should expedite funding for test-bed development and threat-level transformer and EMP/GMD protection hardware testing.

EMP Executive Order activities have promoted the development and demonstration of innovations in grid EMP protection technology including lower-cost shielding materials, modular EMP-hardened substation control buildings and containers, EMP-E3/GMD ground current blocking devices, dual-use EMP/lightning surge arrestors, and high voltage transmission line E1 limiters.

Important milestones remain in the U.S. electric grid's "electromagnetic security" challenge. As previously mentioned, we have not developed the necessary EMP threat-level effects test data base on large transformers and generation stations. Threat level EMP testing of transformers has been limited to small distribution units. Threat level testing of generation stations has only just begun. There have been several analytical studies and low-level tests with optimistic survivability prognostics, but experience dictates that conclusions about system EMP immunity based on analysis and low-level testing are not reliable.[14] Unfortunately, some senior officials in government and industry have accepted and openly endorsed these inconclusive and tenuous analytical results. The DOD program test statistics demonstrate that analytical studies of system EMP effects without follow-on threat-level system testing have a very high likelihood of erroneous conclusions. If analytical studies that predict transformer EMP immunity prove to be incorrect, because of considerable replacement transformer procurement lead times, national recovery periods would be extended from an estimated 30-day minimum to in excess of one year.

Microgrids as an Electric Power EMP Resilience Tool

Recent major power outages in Puerto Rico, California, and Texas have contributed to a large increase in microgrid installations. EMP-hardened microgrids are a helpful tool as part of the previously mentioned bottom-up effort to protect time-urgent high-risk lifeline and national security infrastructure sites. Microgrids offer many advantages that are accelerating their incorporation as primary local power sources. The main benefit is the elimination of unacceptably high risks of extended grid outages by incorporating organic power sources independent of the BES and local electric distribution systems. An important microgrid attribute, in relation to improved grid survivability and recovery, is their inherent islanding (ability to function disconnected from the rest of the grid) capability. If properly designed and installed, microgrid islands continue to function independent of the larger grid during blackout contingencies. In addition to sustaining critical

14 Electromagnetic Effects Comparison Test and Reliability Assessment (ELECTRA) Program, Executive Summary of the ELECTRA Technical Review Group, Defense Nuclear Agency, 1995.

services, they can be helpful in blackstarting the larger electric grid.[15] As a bonus, when completely isolated from the larger grid, microgrids' small footprint makes them immune to EMP-E3 and GMD effects.

However, without intentional protection, microgrids are far from a silver bullet solution to threats and hazards associated with the larger electric power "macrogrid." Because of their organic digital monitoring and control systems, microgrid networks are highly susceptible to EMP and cyberattacks. Furthermore, integration of microgrids into the larger existing electric power grid, without attention to protection engineering, actually increases the vulnerability of the larger grid composite by exacerbating the "vulnerability of complexity."[16] Because microgrid control systems interface with control systems for the larger grid, microgrids provide attack paths into the generation, transmission, and distribution sectors of the larger national grid.[17] Microgrid installations to date have not incorporated protection engineering. Without attention to protection engineering, the proliferation of microgrids makes our composite electricity supply system more vulnerable to EMP and cyber threats. Designed-in protection represents a single digit percentage cost differential. DOD experience indicates that retrofit protection costs run an order of magnitude higher than designed-in protection.

Communications, Data Systems, and Network Resiliency

Telecommunications infrastructure continues to undergo significant transformation. Packet-based internet protocol networks have largely subsumed circuit-switched networks enabling broadband, diverse, scalable packet-based networks, now in the 4th generation and transitioning to 5th generation (5G) technology. There is a continuing dramatic growth in wireless services and applications including the proliferation of base stations and radio-cell tower infrastructure throughout wireless provider service areas.

Dependency on digital mobile phones, Internet communications, and wireless local-area networks support a growing internet of things (IOT) comprising a host of new controlled physical infrastructures including the smart grid, smart buildings and smart homes. This expansion will increase the consequences of EMP/GMD-caused power outages and electronics failures. The rapid proliferation and integration of telecommunications and computer systems and networks have connected infrastructures to one another in a complex network of interdependence. Higher bandwidth wired and wireless systems have increased the capabilities and use of digital automation of life-line infrastructures, including the elec-

15 G. Baker, "Microgrids—A Watershed Moment," *Insight Magazine*, International Conference on System Engineering, June 2020, Vol. 23/ Issue 2.

16 C. Perrow, *Normal Accidents: Living with High-Risk Technologies*, Princeton University Press,1999.

17 G. Baker, "Microgrids—A Watershed Moment," Op. Cit.

tric power systems, water systems, transportation systems, and financial systems. These digital monitoring and control network overlays add a new dimension of EMP risks.

Communication and data network monitoring and control increase the grid's vulnerability to both EMP and cyber debilitation because they introduce new attack vectors exploitable by malefactors. An important case in point is the increased use of Internet-based automation of grid operation as part of smart grid, smart city, and IOT initiatives. To reduce costs, many electric companies, instead of building dedicated monitoring and control data networks, route their data over the Internet. Hackers have used the grid's Internet connectivity to shut down electric power in Ukraine[18] and India.[19] These are important examples of private efficiency creating public vulnerability.[20] To counter this broad movement towards increased vulnerability, we must form public-private partnerships oriented to protecting the public interest. Just as important, we must take steps to provide cost recovery and insurance incentives that encourage private investment in EMP/GMD resilience.

It is important to note that EMP affects the same electronic equipment targeted by cyber-attacks. Conducting Internet paths penetrating infrastructure control systems can also deliver high voltage EMP transients into the same digital devices. And EMP has other paths into equipment as well. EMP is able to bypass cyber security firewalls, air gaps and optical fiber isolation lines by coupling directly to electronic boxes power supply cables. Thus, EMP effects are significantly more ubiquitous than cyber effects since EMP couples to local networks and electronic data and communications systems not linked to the Internet.

Communication and data systems and networks required for grid operation necessarily rise to the top of the DHS priority system identification list. Both normal operation and emergency restoration of the grid in EMP contingencies depend on functional on-site communication systems and the communication/data networks interconnecting grid control centers with generation plants, substations, transmission systems, and distribution systems.[21] The National Security Telecommunications Commission continues to be concerned about the interdependencies between the communications and electric power sectors.

The grid is not alone—the operation and maintenance of all critical infrastructures rely on the larger public switched telephone network (PSTN) which also supports the Internet. These networks also play critical roles during emergen-

18 E-ISAC, Analysis of the Cyber Attack on the Ukrainian Power Grid, March 18, 2016

19 https://www.nytimes.com/2021/02/28/us/politics/china-india-hacking-electricity.html

20 L. Branscomb et al, *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*, National Institute of Standards - George Mason University, Private Efficiency, Public Vulnerability Project, Cambridge Press, 2006.

21 D. Winks, Protecting U.S. Electric Grid Communications from Electromagnetic Pulse, Foundation for Resilient Societies, April 2020.

cies and in reconstituting societal functions following disasters. Several rules of thumb help in ranking the EMP susceptibility of communications systems. Land line networks are the most susceptible to EMP and GMD because of the large number of nodes and long-interconnecting copper lines—or EMP/E1 susceptible regeneration/repeater stations in the case of fiber-optic networks. Though cell phones themselves are likely to be undamaged by EMP, cell phone communications will fail since cell towers are highly susceptible and are interconnected via the land line system. Telephone central offices are also highly susceptible to EMP (and GMD in the case of long line terminal equipment) effects. Failure of long-haul telecommunication systems will prevent local and long-distance telephone service and Internet connectivity. Satellite phones are also likely to fail since satellites down-link to the PSTN through EMP-susceptible terrestrial receiver stations. Some commercial radio and TV stations may continue to operate if they have survivable backup power. Many HAM stations will continue to function. Some first responder hand-held and land-mobile radio (LMR) radio systems will continue to function if they have survivable backup power. Mobile radio base stations and repeaters may be debilitated. Hand-held and vehicle-mounted satellite UHF radios (e.g., military manpack PRC-117 radio) that connect through high-orbit geosynchronous satellites are likely to continue to operate. EMP testing of specific portable and mobile radio systems and associated base stations and repeaters used by first responders is relatively simple and inexpensive and strongly recommended to ascertain their survivability. In general, radio connectivity is much more likely to remain following EMP exposure. Point-to-point radio systems are the most resilient to EMP environments assuming backup power/battery rechargers are available. Given current vulnerabilities, it is not prudent to rely on network operations center or emergency operations station land-line connectivity.

There is some good news regarding EMP/GMD protection practicality and cost. The public switched telecommunications network (PSTN) is the foundational backbone for U.S. communications. The Telecommunications Act of 1996 opened local PSTN service to competition. The legislation requires incumbent carriers to allow their competitors to have open access to their networks. As a result, carriers are concentrating their assets in collocation facilities known as telcom hotels, collocation sites, or peering points. Internet Service Providers (ISPs) have also gravitated to these facilities to reduce costs. This has curtailed the proliferation of data centers and reduced the requirement for and cost of laying new cable. This means fewer facilities and a lower number of interconnecting cables that require EMP/GMD protection.

Cost Recovery Mechanisms Essential

Achievement of privately-owned infrastructure resilience is unlikely without the establishment of EMP protection cost recovery mechanisms. Under present Fed-

eral Energy Regulatory Commission (FERC) rules, BES protection cost recovery is possible only for the transmission portion of the grid. Generation operators may not recover costs for resilience expenses. Legislation is needed to expand cost recovery provisions to include the generation portion of the electric power grid. Some strategies for cost recovery could include identification of "resilience" as an investment justification, modification of tax credits for microgrids and renewables to include resilience, enactment of federal legislation to provide block grants to states for critical infrastructure protection and addressing EMP under the "multi-hazard" rubric to justify protection from the combination of floods, hurricanes, earthquakes, EMP, Solar Storms, and other hazards.

In addition, Tier 1 national security and infrastructure customers—including defense facilities, key data centers, water and wastewater facilities, emergency responders, hospitals, and nuclear power plants—may request firm electric power delivery that requires high reliability and resilient supply and delivery. These customers may rely upon federal or state or municipal appropriations so the "customer pays" principle applies when specific customer priority service is a necessity. Cost savings can be achieved by leveraging existing new builds and replacements to install hardened equipment to minimize the incremental expense of retrofit hardening.

At this point, examples of regulatory agencies specifying or incentivizing EMP/GMD protection of critical infrastructures are scarce. The Energy sector has developed reliability standards through the North American Electric Reliability Corporation (NERC) to protect against GMD including NERC Reliability Standard TPL-007-4 and EOP-010-1. Also, Maine and Virginia have passed electric grid laws that include EMP/GMD disaster mitigation. The federal government must demonstrate a greater interest in regulating or incentivizing adoption through cost recovery, EMP resilience will remain a low priority among critical infrastructure stakeholders.

The Way Forward

EMP has for too long been considered prohibitively difficult and expensive to address. Such is not the case. The major challenge has been the ubiquity of EMP effects. This can be overcome by defining a minimum essential set of systems and network nodes requiring protection and work-around procedures to restore systems that are intentionally allowed to fail. We know how to harden systems. EMP can be viewed and treated as a facility-level electromagnetic interference (EMI) engineering problem. Critical systems must make maximum use of shielded compartments connected with optical fiber. Since hardening costs are proportional to the floor space occupied by electronic boxes and racks, there is a premium on compressing the space occupied by essential electronics. Shielded spaces and cabinets can be fitted with simple, built-in self-monitoring or 'push-button/read

meter' shielding effectiveness test devices to ensure protection is surveilled and maintained. Box-level protection is feasible if box EMI field exposure and penetration injection test requirements are adjusted up to 50 kV/m and corresponding coupled current and voltage levels (specifications will be cable dependent and can be handled with look-up tables as in IEC Standard 61000-2-10). In particular, the issuance of an official unclassified EMP protection handbook is long overdue. DHS has been working this issue and is close to a final product for communication and data facilities and networks and associated backup power.

The foundational Report of the President's Commission on Critical Infrastructure Protection of 1997 (PCCIP Report) has not helped the case for national electromagnetic effects resilience, including EMP, GMD and intentional electromagnetic interference (radio-frequency weapons, high power microwave weapons, ultra-wideband weapons, jamming devices, etc.). The report divided infrastructure threats into two categories: 'physical security' and 'cyber security.' This categorization has governed protection program objectives and budgets for over two decades. The 'electromagnetic security' category and associated highly asymmetric effects due to the large areas affected by single events does not fit neatly under the PCCIP's physical security or cyber security definitions. Electromagnetic Security has fallen through the cracks, largely unaddressed in national security planning and system/network design and operation. For instance, EMP did not make the list of DHS' early compilation of the top one-hundred U.S. threats. "Electromagnetic Security" must be included as a separate category in national security strategic planning and budget authorization documents.

One cannot expect instant gratification in the quest for national electromagnetic security. It will take time to delimit the systems that absolutely must survive EMP and GMD. Hardened microgrids are likely the most effective near-term solution for electric power protection. FERC has identified the most essential substations in the bulk electric power grid—attention to these will greatly improve the recoverability, if not the survivability of the transmission system. From a communications standpoint, the regional control centers that tie the generation, transmission, and distribution elements of the electric power grid together are the top priority systems for protection. This is due to their role in controlling the grid during normal operations and during grid restoration including grid isolation, power re-routing, and general situational awareness during grid outages. Control center protection engineering hardware and procedures are available and already demonstrated on two major control centers within the Center Point and Dominion Energy systems. There are approximately 300 major centers across the United States. Federal incentives to protect and to perform testing of these centers and their associated communication and control networks are well advised.

In summary, Presidential Executive Order 13865 has spurred substantial national attention to electromagnetic security vis-à-vis nuclear EMP and solar

GMD. The Executive Order provisions are now legally binding under the 2020 National Defense Authorization Act. The electric power grid, communications, and water sectors are at the forefront of national CI electromagnetic security efforts. It is impractical to harden all critical infrastructure, but careful screening to identify key life/enterprise-supporting and national security systems will enable affordable EMP preparedness. Thanks to DOD's attention to EMP effects and hardening since the 1960s, including the development of standards, protection engineering solutions are known, implemented, and validated for data and communication equipment and centers. Achieving EMP/GMD resilience of the national grid will necessarily involve combined top-down and bottom-up efforts. The top-down approach focuses on protecting generation and transmission systems (BES) under federal government jurisdiction. The bottom-up effort will protect electric distribution system and its CI customers which are under the jurisdiction of State and local governments. Hardened microgrids are a helpful tool as part of the bottom-up effort to protect time-urgent high-risk lifeline and national security infrastructure sites. Protection of the key nation-wide communication networks including the PSTN and Internet is aided by the collocation of network electronic equipment and line terminations in multi-provider network operation centers. Key remaining challenges include (1) priority system identification and down-selection, (2) validating protection methods for high voltage grid systems, (3) filling the present EMP threat-level test data void on large transformers and generation stations, and (4) the establishment of EMP protection incentives and cost recovery mechanisms.

Acronyms

BES	Bulk-power Electric System
CONUS	Contiguous United States
DHS	Department of Homeland Security
DOD	Department of Defense
EMI	Electromagnetic Interference
EMP	Electromagnetic Pulse
FERC	Federal Energy Regulatory Commission
GMD	Geomagnetic Disturbance
GSU	Generator Step-up Transformer
IOT	Internet of Things

ISP	Internet Service Provider
NDAA	National Defense Authorization Act
NSTAC	National Security Telecommunications Advisory Council
PSTN	Public Switched Telephone Network
RTO	Regional Transmission Organization

Capsule Bio

Dr. George Baker is emeritus professor of applied science at James Madison University (JMU), where he also directed the university's Institute for Infrastructure and Information Assurance during 2000-2012. He recently retired from the National Security Council staff, where he coordinated federal interagency implementation of EMP executive order 13865 tasking. From 1999-2000, Baker served as a senior scientist at Northrop-Grumman, advising Defense Threat Reduction Agency (DTRA) nuclear effects R&D programs. He served as Director of DTRA's Springfield Research Facility from 1996-99, a national center for critical system all-hazards vulnerability assessment and protection guidance. Baker's organization developed the JCS Force Protection assessment program. From 1994-1996, he directed the Defense Nuclear Agency's Innovative Concepts Division, managing advanced weapon concept development and protection technology research. From 1987-1994, Baker led the Defense Nuclear Agency's electromagnetic effects programs to protect strategic systems and develop DOD's EMP guidelines and standards. He now applies lessons-learned from DOD experience to critical national infrastructure assurance and community resilience. He has consulted in the areas of critical infrastructure protection, EMP and geomagnetic disturbance (GMD) protection, nuclear and directed energy weapon effects, and risk assessment for customers including DOD, DOE, DHS, the White House, National Guard units, the National Park Service, SAIC, George Mason University, Oregon State University, and Defense Group Inc. During 2001-2008 and 2016-2017 he served as senior advisor to the Congressional EMP Commission. From 2011-2019 he served on the Board of Directors of the Foundation for Resilient Societies, the Board of Advisors for the Congressional Task Force on National and Homeland Security and the JMU Research and Public Service Advisory Board. Degrees include M.S., Physics (University of Virginia) and Ph.D., Engineering Physics (U.S. Air Force Institute of Technology).