



Statement for the Record, July 21, 2009

Hearing before the Subcommittee on Emerging Threats, Cybersecurity, Science and Technology

Respectfully submitted by: Emprimus LLC

**1660 S. Hwy. 100, Suite 130
Minneapolis, MN 55416**

Chairwoman Clarke, Ranking Member Lungren, Chairman Thompson, Ranking Member King, and Members of the Subcommittee:

Thank you for the opportunity to share with you our thoughts about the present vulnerability of the U.S. electric grid and other critical civilian infrastructure to growing electromagnetic threats, and our recommendations for steps towards remediation of these threats. Emprimus is deeply concerned about our national infrastructure electrical, electronic, and cyber vulnerabilities in a number of areas, and has already been involved in several discussions with Congressional members and their staffs, and other agency personnel about these issues, as well as providing briefings to relevant industry and technical associations in recent months. Emprimus has a multi-disciplined background which includes a private testing program to evaluate and understand the vulnerability of many types of civilian electronic equipment to these growing threats, as well as new ways to remediate them.

We strongly support legislation to amend the Federal Power Act to provide additional authorities to adequately protect the critical electric infrastructure against cyber attack and the related intentional electromagnetic interference (IEMI) attacks, as well as hardening the electric grid against high altitude electromagnetic pulse (EMP) and severe geomagnetic storms. For conciseness in this record, we will generically refer to all electromagnetic threats as "EMP." As we will show, all three of these threats are related in that they have similar effects and share common remediation solutions. It is important to note at the outset that EMP is also a cyber threat just as surely as internet hackers are, since data states can be destructively altered.

1. What are the severe electromagnetic threats to our electric system and other critical infrastructure?

Every year, the modern infrastructure of the U.S. becomes increasingly dependent on integrated circuit-based electronic control systems, computers, servers and burgeoning masses of electronically stored data. The emerging threat and growing use of non-nuclear EMP/IEMI (Intentional Electromagnetic Interference, including Radio Frequency {RF} weapons) poses grave dangers to all of our civilian infrastructure, including our national electric grid, civilian facilities' data and data assets, and can damage computer systems, their electronic equipment and the data they contain, control and monitoring systems, and support systems which would impede operations of most critical civilian infrastructure installations. Support systems at risk range from security systems to communication links to fire protection to all HVAC systems.

For instance, recent research and testing shows how power distribution can be shut down for a multi-state area by mobile non-nuclear EMP attacks. Major metropolitan areas in the U.S. have a number of critical choke points. For example, some electrical substations in each area of the country connect a large amount of electric generation to the bulk electric transmission system, and similar electrical substations are used to connect the transmission system to the metropolitan distribution system. A mobile non-nuclear attack perpetrated by terrorists or other parties in an innocent looking truck at the typically unguarded perimeter of a single substation would cause connection faults and trips, resulting in dropping generators off line similar to recent blackouts in New York and Florida. A coordinated attack at several of these substations could lead to a cascading collapse condition, leading to prolonged large multistate power outage conditions. A multi-city coordinated attack could have an even more serious national effect. With proper attention to shielding and filtering of substation electronics controls, communications equipment, and data centers as part of a mandated improvement program, the impacts of these intentional EMP events can be minimized.

The military has shielded their facilities for decades against EMP. Now, high levels of EMP can be delivered locally by either hand held devices, or via more powerful vehicle borne weapons, and create disruption and damage similar to that caused by high altitude EMP, but on a local scale. The threat of a severe geomagnetic storm is always with us, and will occur at some time in the future with near certainty. (A solar event similar to the 1859 storm would cause catastrophic damage to our modern electricity based infrastructure.) The recent Quebec grid collapse as a result of a serious solar storm has resulted in Canadian action to improve its grid.

The following chart shows how all three types of electromagnetic threats to our infrastructure are related with regard to their damage and disruption effects.

	Damage to Electric Grid Transformers	Damage to Grid Electronic Controls and Data	Damage to Other Infrastructure Electronics and Data
High-altitude Electromagnetic Pulse (EMP)	Yes, National Scale	Yes, Serious	Yes, Serious
Intentional Electromagnetic Interference, or Non-nuclear EMP	Local or Regional Effects	Yes, Serious Local	Yes, Serious Local
Severe Geo-magnetic Storms	Yes, Regional or National Scale	Sporadic	Sporadic

This chart shows how the impacts of these threats are related. Fortunately, appropriately mandated national action can significantly reduce the impacts of all three threat classes.

The International Electrotechnical Commission (IEC)

has defined non-nuclear EMP/IEMI as the “intentional malicious generation of electromagnetic energy introducing noise or signals into electric and electronic systems thus disrupting, confusing, or damaging these systems for terrorist or criminal purposes.” The insidious aspect of this class of EMP for the energy sector and other key sectors of our national infrastructure is that it attacks both cyber and physical security aspects of our electronics-based systems in manners that can completely circumvent firewalls, tier structures, layered networks, passwords, physical barriers, security procedures, etc. Unlike traditional cyber threats to data security, non-nuclear EMP may be extremely covert and difficult to detect and trace with forensics, and with the ability to impede digital forensics by corrupting the data. There are remediation approaches to help diminish this threat class if appropriate steps are taken.

2. What are the effects of an EMP event on the electric system?

Non-nuclear EMP attack As demonstrated in the example above of a relatively modest attack by a small number of individuals on several critical electric power substations, substantial damage and disruption can be inflicted by the use of these uncontrolled and easy to deploy electromagnetic weapons. The U.S. Navy has shown how plans for many of these devices are available on the internet, has tested and demonstrated the vulnerability of computer and SCADA systems, and has demonstrated the fabrication and use of such a device built with a total parts cost of \$500.00. These man-portable or vehicle borne weapons are becoming a modern tool of those wishing to conduct highly asymmetrical warfare, including disgruntled employees, criminals, extremists, and terrorists. These devices can be deployed against electric power substations and other electronics, and in fact against all 18 segments of the DHS sectors of critical civilian infrastructure with similar results.

High altitude EMP attack A high altitude EMP event detonated several hundred miles above the center of the contiguous U.S. would cause catastrophic damage to the present national electrical grid, as was detailed by the recent Congressional EMP Commission: “Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack,” April 2008. An EMP event of this type has an initial fast burst lasting nanoseconds that will damage or destroy most modern electronics within line of sight that are based on integrated circuitry, and a slower burst lasting up to several minutes that will create very large voltages over hundreds and thousands of miles that will result in disastrous damage to the high voltage transformers and electronics that power our national electric distribution system. As the EMP Commission states, “The electromagnetic pulse generated by a high altitude nuclear explosion is one of a small number of threats that can hold our society at risk of catastrophic consequences. The increasingly pervasive use of electronics of all forms represents the greatest source of vulnerability to attack by EMP. Electronics are used to control, communicate, compute, store, manage, and implement nearly every aspect of United States (U.S.) civilian systems. When a nuclear explosion occurs at high altitude, the EMP signal it produces will cover the wide geographic region within the line of sight of the detonation. This broad band, high amplitude EMP, when coupled into sensitive electronics, has the capability to produce widespread and long lasting disruption and damage to the critical infrastructures that underpin the fabric of U.S. society.” This is not a short duration problem: the high voltage grid transformers that will be destroyed have few spares, little commonality, and most are now manufactured offshore. Lead times for small quantities of these transformers are years, but hundreds or thousands would be destroyed.

Severe geomagnetic storms The impact on electric power transformers deployed at the ends of our long high voltage transmission lines would be essentially the same as that from a high altitude EMP event described above. The geomagnetic induced currents (GIC) from these events will also generate high, damaging voltage surges over any long conductive paths (communications, telecom, data lines, etc.) leading to computer systems, data storage, and any other electronic equipment. An expert in GIC has indicated that uninterruptable power supplies are especially vulnerable. An 1859-class event would shut down most of our grid for years, if our critical transformers remain unprotected.

3. What technological fixes are required to secure infrastructure from an EMP event?

Electronic and data dependent infrastructure The 18 Department of Homeland Security sectors of Critical non-military Infrastructure all have a vital dependence on digital data, electronic sensing, computing, controls, and data storage that can be corrupted and/or damaged by both high altitude EMP and non-nuclear EMP. It is important to point out that these threats are CYBER threats, since they can corrupt and destroy data just as surely as the more publicized internet hacker attacks we are so familiar with these days. In fact, EMP is probably more insidious, since these attacks leave no network footprints and destroy evidence amenable to

digital forensics, and they can cause physical damage to the electronic equipment attacked. It is conceivable that EMP could be used to cover up traditional cyber attacks. Critical equipment in the DHS Critical Infrastructure segments such as data centers, supervisory control and data acquisition (SCADA) systems, process control equipment, etc. can be protected by appropriate electromagnetic shielding, filtering, and security procedures, along with enhanced threat detection. It is especially important that facilities responsible for meeting regulatory data retention requirements rapidly acquire this protection, especially trading institutions and banking data centers. The 2008 EMP Commission Final Report has much more detail on the effects of EMP on telecommunications, banking, refineries and pipelines, and other infrastructure, recommending that mandated fixes proceed promptly.

High voltage transformers The national power grid high voltage transformers must be remediated to withstand the huge direct current voltages they would be exposed to in a high altitude EMP event or severe geomagnetic storm. The 2008 EMP Commission Final Report has a number of specific recommendations regarding transformer protection, improving grid communications and control, safer islanding of grid segments (permitting a damaged portion of the grid to be safely isolated), and other key remediations. Some of these critical fixes can be started immediately and at relatively low cost, especially with regard to high voltage transformer protection. These protections are needed to protect against severe geomagnetic storms, as well as EMP, since at least a severe storm will occur sooner or later.

4. Why does the modernization of the American electric grid create new vulnerabilities that may not have existed before?

There are several factors that are working to increase the vulnerability of our critical electric grid.

Interconnectivity Heavy reliance on interconnectivity to meet peak load demands has increased the probability of cascading failures in the event of an EMP event. This is related to the existence of choke points or critical substations which present attractive asymmetrical targets.

Longer transmission lines Increasing distances encourage use of very high voltage transmission of power from generation source to point of use, and both the high voltage and distance make the system more susceptible to the high altitude EMP and geomagnetic storm threats.

Renewable power sources As more long distance lines are added to deliver power from renewable sources of wind and solar located in sparsely populated areas to distant high population density areas, the exposure of the grid to high altitude EMP and geomagnetic storm damage will be significantly increased. Intelligent planning now can mitigate this danger.

Smart grid The addition of “smart grid” electronic processing and communications between users and generation sources adds many additional points of failure to the operation of the grid if it is attacked by an EMP event.

Electric utility operation Electric utility data centers and control centers for grid operation, customer account management, and business management including regulatory data retention requirements are highly dependent on the operation of electronic equipment, which is at serious risk of data corruption and equipment damage from the fast EMP transients and from more localized EMP/IEMI attacks.

Critical Substations These substations transmit huge blocks of power from large generating plants which, if the controls are damaged, could disrupt large multi-state areas.

As reported by the EMP Commission, each of these vulnerabilities can be greatly diminished by timely action, but the solutions need to be initiated now.

5. Why is the U.S. electric grid different from other nations?

The size and technology of the U.S. electric grid differentiates it from most other third world nation grids. For example, differentiating features include

- Longer transmission lines due to lower population density and large area
- More critical substations
- More prevalent conversion from coal to natural gas, in more vulnerable automated and unmanned facilities
- Many more high voltage transformers susceptible to EMP damage

As described previously, each of these factors contributes to increased EMP risk.

In contrast to most other developed countries that have one or two electrical power entities, the U.S. has over four hundred transmission-owning entities, greatly complicating coordinated remediation efforts. Also, the R&D and electrical infrastructure capital improvement expenditures have been in serious decline in recent years. These factors complicate implementing a coordinated remediation of our nation’s electrical power system against the three EMP threats. It will require additional federal authority to mandate swift and coordinated action, along with appropriate federal funding to initiate these appropriate steps.

6. What is the cost of securing our electric and other critical infrastructure from an electromagnetic event such as EMP, severe geomagnetic storms, or non-nuclear EMP/IEMI?

On June 10, 2009, Emprimus gave a briefing on the subject at a meeting sponsored by the National Defense University and the National Defense Industrial Association on Capitol Hill. The following estimates for infrastructure protection were presented:

**Requested Congressional Action
And Funding for Critical
Infrastructure Remediation**

**Minimal Congressional Action and Funding
For the Most Critical Facilities in Each
Infrastructure**

Protect High Voltage Transformers and Critical Substations	\$1B
Pipelines, Water, and Waste Water	\$1B
Utilities' Data Centers and Control	\$2B
Smart Grid Remediation For Electromagnetic Threats	\$500M
911 & State Emergency Ops (EOC) State Fed and County Data Centers	\$2B
Key Financial Data Centers	\$2B
Infrastructure Research	\$500M
EMP Threat Detectors and other External Threat Security	\$750M

Most Critical HV Transformers	\$150M
Pipelines, Water, and Wastewater	\$100M
Utility Data Centers and Controls	\$150M
Key Smart Grid Remediation	\$100M
911 & State Emergency Ops (EOC) State Fed and County Data Centers	\$200M
Critical Financial Data Centers	\$150M
Key Infrastructure Research	\$75M
EMP Threat Detectors and other External Threat Security	\$75M

The first column shows the levels required to reduce our infrastructure risks to acceptable levels from the physical and cyber threats imposed by the subject electromagnetic threats, and the second column shows a minimal initial program to start actions on the most critical infrastructure reinforcement needs. Although it partitions the problem slightly differently, the Congressional EMP Commission Final Report of April, 2008, has similar numbers for the electric supply portion of the infrastructure hardening. The highest priority objective is to protect a subset of the most critical national infrastructure so that minimal services can be restored after a severe event to allow recovery to begin. The initial costs are obviously a function of the level of critically definition, numbers of protected facilities, and levels of protection.

The Final Report of the Congressional Commission on the Strategic Posture of the United States, May 2009, states that:

Findings: **“The United States is highly vulnerable to attack with weapons designed to produce electromagnetic pulse effects.”**

Recommendations: **“EMP vulnerabilities should be reduced as the United States modernizes its electric power grid.”**

Mme. Chairwoman, it is our hope that this has been useful information for the Subcommittee on the serious national issue of EMP. Again, we strongly support legislation to amend the Federal Power Act to provide additional authorities to adequately protect the critical electric infrastructure against cyber attack and the related non-nuclear EMP/IEMI attacks, as well as hardening the electric grid against high altitude EMP and severe geomagnetic storms. We would look forward to answering any questions you may have, and we thank you, Ranking Member Lungren, and the Members of the Subcommittee for your support in addressing this electric power vulnerability and the broader issue of the vulnerability of our critical national infrastructure sectors to these electromagnetic Achilles heels.

Respectfully submitted,

George Anderson, Founder and Chairman
Gale Nordling, CEO and President
Emprimus LLC
Minneapolis