AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

THE EMP THREAT: THE STATE OF PREPAREDNESS AGAINST THE THREAT OF AN ELECTROMAGNETIC PULSE (EMP) EVENT

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY

AND THE

SUBCOMMITTEE ON THE INTERIOR

OF THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

MAY 13, 2015

Serial No. 114–42

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.fdsys.gov
http://www.house.gov/reform

U.S. GOVERNMENT PUBLISHING OFFICE

96–952 PDF WASHINGTON : 2015

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

JASON CHAFFETZ, Utah, *Chairman*

JOHN L. MICA, Florida
MICHAEL R. TURNER, Ohio
JOHN J. DUNCAN, JR., Tennessee
JIM JORDAN, Ohio
TIM WALBERG, Michigan
JUSTIN AMASH, Michigan
PAUL A. GOSAR, Arizona
SCOTT DESJARLAIS, Tennessee
TREY GOWDY, South Carolina
BLAKE FARENTHOLD, Texas
CYNTHIA M. LUMMIS, Wyoming
THOMAS MASSIE, Kentucky
MARK MEADOWS, North Carolina
RON DESANTIS, Florida
MICK MULVANEY, South Carolina
KEN BUCK, Colorado
MARK WALKER, North Carolina
ROD BLUM, Iowa
JODY B. HICE, Georgia
STEVE RUSSELL, Oklahoma
EARL L. "BUDDY" CARTER, Georgia
GLENN GROTHMAN, Wisconsin
WILL HURD, Texas
GARY J. PALMER, Alabama

ELIJAH E. CUMMINGS, Maryland, *Ranking Minority Member*
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
MATT CARTWRIGHT, Pennsylvania
TAMMY DUCKWORTH, Illinois
ROBIN L. KELLY, Illinois
BRENDA L. LAWRENCE, Michigan
TED LIEU, California
BONNIE WATSON COLEMAN, New Jersey
STACEY E. PLASKETT, Virgin Islands
MARK DESAULNIER, California
BRENDAN F. BOYLE, Pennsylvania
PETER WELCH, Vermont
MICHELLE LUJAN GRISHAM, New Mexico

SEAN MCLAUGHLIN, *Staff Director*
DAVID RAPALLO, *Minority Staff Director*
ANDREW R. ARTHUR, *National Security Subcommittee Staff Director*
WILLIAM MCGRATH, *Interior Subcommittee Staff Director*
SHARON CASEY, *Deputy Chief Clerk*

Subcommittee on National Security

RON DESANTIS, Florida, *Chairman*

JOHN L. MICA, Florida
JOHN J. DUNCAN, JR., Tennessee
JODY B. HICE, Georgia
STEVE RUSSELL, Oklahoma, *Vice Chair*
WILL HUR, Texas

STEPHEN F. LYNCH, Massachusetts, *Ranking Member*
ROBIN L. KELLY, Illinois
BRENDA L. LAWRENCE, Michigan
TED LIEU, California

Subcommittee on the Interior

CYNTHIA M. LUMMIS, Wyoming, *Chairman*

PAUL A. GOSAR, Arizona
BLAKE FARENTHOLD, Texas
KEN BUCK, Colorado, *Vice chair*
STEVE RUSSELL, Oklahoma
GARY J. PALMER, Alabama

BRENDA L. LAWRENCE, Michigan, *Ranking Member*
MATT CARTWRIGHT, Pennsylvania
STACEY E. PLASKETT, Virgin Islands
JIM COOPER, Tennessee

CONTENTS

	Page
Hearing held on May 13, 2015	1

WITNESSES

Mr. George Baker, Professor Emeritus, James Madison University, CEO of Baycor	
Oral Statement	5
Written Statement	8
Dr. Peter Vincent Pry, Executive Director, Task Force on National and Homeland Security	
Oral Statement	21
Written Statement	23
Mr. Mike Caruso, Director of Government and Specialty Business Development ETS-Lindgren	
Oral Statement	49
Written Statement	51

APPENDIX

Walpole Fire Department Research Paper 2012	70
Submission of William Graham, Commission to Assess Threat to U.S. From EMP Attack	71
Submission of William Radasky, Metatech Corporation	75
Submission of Thomas Popik, Resilient Societies	80
Opening Statement from Interior Ranking Member Brenda Lawrence	85
Opening Statement from Congressman Trent Franks	87

THE EMP THREAT: THE STATE OF PREPAREDNESS AGAINST THE THREAT OF AN ELECTROMAGNETIC PULSE (EMP) EVENT

Wednesday, May 13, 2015

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON NATIONAL SECURITY, JOINT WITH
SUBCOMMITTEE ON THE INTERIOR,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, D.C.

The subcommittees met, pursuant to call, at 2:20 p.m., in Room 2154, Rayburn House Office Building, Hon. Ron DeSantis [chairman of the subcommittee on National Security] presiding.

Present for Subcommittee on National Security: Representatives DeSantis, Duncan, Hice, Russell, Lynch, Lieu, and Kelly.

Present for Subcommittee on the Interior: Representatives Lummis, Gosar, Buck, Palmer, and Lawrence.

Mr. DESANTIS. The Subcommittees on National Security and Interior will come to order. Without objection, the chair is authorized to declare a recess at any time.

The state of preparedness against the threat of an electromagnetic pulse is the subject of today's hearing. An electromagnetic pulse could be created through an attack from a missile, nuclear weapon, radio frequency weapon, or geomagnetic storm caused by the sun. Fallout from an EMP event, either man-made or natural, could be extremely significant ranging from the loss of electrical power for months, which would deplete energy sources of power such as emergency batteries and backup generators have cascading consequences for supplying basic necessities such as food and water, and result in loss of life.

The electrical grid is necessary to support critical infrastructure, supply and distribution of food, water, and fuel, communications, transportation, financial transactions and emergency and government services. Significant damage to the electrical grid during an EMP event would quickly and significantly degrade the supply of these basic necessities.

EMPs can also be caused by solar storms, also referred to as geomagnetic disturbances, which are basically an everyday occurrence, they just doesn't always hit the Earth. Two significant storms that did enter the earth's atmosphere occurred in 1859 and 1921, respectively. Given the limited use of electricity in the mid-19th and early 20th centuries, the impact on society was relatively minimal.

Today however, society depends heavily on a variety of technologies that are vulnerable to the effects of intense solar storms.

Scientists predict that these storms impact the Earth once every 100 to 150 years. So it's not a question of if, but a question of when.

The occurrence today on an event like the 1921 storm could result in large scale and prolonged blackouts affecting more than 100 million people. The National Academy of Sciences estimates the cost of damage from the most extreme solar weather at $1 to $2 trillion with a recovery time of 4 to 10 years. The cost from even short-term blackouts are significant.

In July of 1977, a blackout in New York that lasted only one day resulted in widespread looting and the breakdown of law through many New York neighborhoods. The blackout cost approximately $346 million and nearly 3,000 people were arrested during a 26-hour period. In August of 2003, more than 200 power plants shut down as a result of the electricity cut off caused by cascading failure. The blackout affected Ohio, New York, Maryland, Pennsylvania, Michigan and parts of Canada. Although relatively short in duration, the blackout's economic cost was between $7 billion and $10 billion due to food spoilage, lost production, overtime wages and other related costs.

To look at this threat, Congress has created two EMP commissions which reported their findings in 2004 and 2008. Based in large part on their recommendations, a bill has been introduced in every Congress since 2009 to strengthen protection of the electrical grid by mitigating the effects of an EMP. Some bills have passed the House but no bills have yet become law.

Congress is not alone in its assessment of the EMP threat. State governments, such as in New York and Massachusetts have taken action themselves to protect portions of the electrical grid located within their respective States. Even some individual utilities have correctly assessed their vulnerability to EMP and hardened a few of their critical electrical control centers.

The Department of Defense recently decided to move the North American Aerospace Defense Command, NORAD back inside Cheyenne Mountain in Colorado because the mountain is EMP hardened and would allow the military to sustain communications and homeland defense operations despite an EMP event.

One of our witnesses here today, Dr. Peter Pry, wrote in The Wall Street Journal earlier this month about the military's decision and rightly surmised, "The Pentagon was wise to move NORAD back into Cheyenne Mountain, but how are the American people to survive?" The Department of Homeland Security, the Federal agency responsible for protecting the American citizens, is not doing enough to lead an interagency effort to mitigate the impact of an EMP event, leaving vast populations of Americans vulnerable to the effects of an EMP.

Lastly, the draft executive order by the National Space Weather Strategy was released for comment earlier this month by the White House Office of Science and Technology Council. This order is necessary and clearly within the constitutional mandate to provide for the common defense, but it is an outline of goals, not what is needed. A strategy with priorities and a blueprint for how to reliably mitigate adverse solar weather.

It is essential that state and national leaders have adequate plans at hand to determine how best to respond to EMP threats as they arrive. As such, it is critical that a scenario focused on the EMP threat be included in national planning scenarios by the Department of Homeland Security. This is precisely the directive included in the Critical Infrastructure Protection Act sponsored by my good friend, Congressman Trent Franks, who will be here with us today later to discuss the importance of the EMP issue. His bill would require DHS to take the lead for researching for how to best prepare and protect the American citizens from the threat of an EMP event.

Trent is also the leading sponsor on legislation such as the Secure High-Voltage Infrastructure for Electricity from Lethal Damage Act, the SHIELD Act, which again, seeks to strengthen America's hand against an EMP attack.

I look forward to hearing Trent's thoughts on this issue when he's able to come as well as our other witnesses because this is an important issue and there are things our government can do to address it right now. And with that, I recognize the ranking member, the gentleman from Massachusetts for 5 minutes.

Mr. LYNCH. Thank you, Mr. Chairman. I'd like to thank you and also Chairwoman Lummis for holding the hearing, this hearing to examine our state of preparedness against the threat of a Electromagnetic Pulse Event, also known as a EMP.

As well, I would like to thank our colleague, Mr. Franks of Arizona, who will, as you say, join us shortly and also, our other witnesses on the panel today for helping us with our work.

As set forth in President Obama's 2015 national security strategy, a comprehensive national security agenda must prioritize efforts to address the top strategic risk to the U.S. interests, including the possibility of a catastrophic attack on U.S. critical infrastructure.

Similarly, the strategic plan developed by the Department of Homeland Security provides that we must enhance security for our Nation's critical infrastructure against the threat of a terrorist attack by identifying key vulnerabilities and addressing them through the implementation of appropriate technology.

In support of our shared responsibility to protect America against attack, we must make every effort to examine the extent of potential threats such as an electromagnetic pulse event to our homeland security. Now, this oversight is even more critical, given that the current budgetary climate requires Congress to make very difficult choices in determining Federal agency spending.

Not only is the Federal Government still operating under sequestration, but unfortunately, Congress recently passed a budget blueprint that contemplates cutting nondefense spending, including our Homeland Security budget that could be helpful on this issue by nearly $500 billion below sequestration level spending caps.

While government officials, scientists and other experts may disagree on the imminence of Electromagnetic Pulse event, the EMP Commission established by Congress in 2001 to assess the threat of an EMP attack reported that our national electric grid and other U.S. Critical infrastructure could be significantly disrupted by a sudden and high-intensity energy field burst. Now as the chairman

noted, this could be large in scale and produced by nuclear explosion, it could also be created through the use of batteries, reactive chemicals and other nonnuclear devices, or be the product of a natural magnetic storm.

According to the Commission's 2008 report, "Because of the ubiquitous dependence of U.S. Society on electrical power systems, its vulnerability to an EMP attack, coupled with the EMP's particular damage mechanisms creates the possibility of a long-term catastrophic consequence." A 2012 research paper prepared by a Fire Department in my congressional district—and I'd like to ask unanimous consent to submit the report by Deputy Chief Michael K. Laracy, Sr., from the wonderful town of Walpole, Massachusetts, he's the deputy fire chief there. The title is "Potential Impacts of Electromagnetic Pulse Attacks on Fire and EMS Delivery Services for the Walpole Fire Department."

Mr. DESANTIS. Without objection, so ordered.

Mr. LYNCH. Thank you. In response to such concerns, the House passed H.R. 3410, the Critical Infrastructure Protection Act, by a voice vote at the end of last year. This bill introduced by our friend, Mr. Franks from Arizona, sought to require the Department of Homeland Security to include the EMP threat in its national planning scenario.

While the bill did not pass the Senate, DHS has indicated that the threat of an EMP attack is very much on its radar during recent congressional testimony. Ms. Suzanne Spaulding, the Under Secretary for the National Protection and Programs, indicated that the DHS is currently partnering with private sector entities in the electronic sector to determine how best to address the EMP threat. So I look forward to discussing the issue with our witnesses in order to examine what additional steps we might take in order to better safeguard our national electric grid and other critical infrastructure. Thank you, Mr. Chairman and I yield back the balance of my time.

Mr. DESANTIS. I thank the gentleman from Massachusetts. I ask unanimous consent that enter into the record a letter from Dr. William Graham who is chairman of the 2008 EMP Commission, a letter from Dr. William Radasky, president of Metatech Corporation and leading EMP expert for more than 50 years and a letter, fax sheet and cost estimate model from Thomas Popik, chairman of the Foundation for Resilient Societies. Without objection so ordered.

Mr. DESANTIS. I now recognize the chairwoman of the Natural Resources Subcommittee, Mrs. Lummis, for 5 minutes.

Mrs. LUMMIS. Thank you, Chairman DeSantis for spearheading this hearing. And I also want to thank ranking member, Ranking Member Lynch, thanks for your participation and involvement in this hearing to examine the important issue of electrical grid preparedness in the event of an electromagnetic pulse caused by an attack or a solar storm hitting the Earth.

The threat to the grid infrastructure is real and the potential for devastating impacts needs to be examined. Solar flares have resulted in numerous incidents; the Carrington event of 1859, which at the time, only affected telegraph systems. To be honest, I don't remember the Carrington event personally, I was a mere child at the time. That was a little joke. But I do remember the 1989 geo-

magnetic storm that disrupted radio signals and satellite damage and knocked out the power grid in Quebec. The grid is a critical piece of national infrastructure that contributes to the most basic daily needs of Americans, as well as business and government.

Given the threat presented to this critical infrastructure, I agree with Chairman DeSantis that the Federal Government needs to take the EMP threat seriously by including it in DHS national planning scenario. That's why I support Congressman Trent Franks' Critical Infrastructure Protection Act. This important bill takes a step forward towards protecting our grid against an EMP threat. I note that it passed the House last Congress, and I appreciate all the hard work that Congressman Trent Franks has done on this issue.

The Federal Government needs to follow the lead of State-based utilities and harden the grid against an EMP threat. As we will hear today, the entirety of the Nation's grid is not prepared to deal with a variety of threats. It is important that the Federal Government realize this and takes the necessary steps to protect the grid. I welcome the testimony of our witnesses today. I look forward to hearing more about what our country needs to do to protect against the threats of EMPs. Mr. Chairman, thank you, I yield back.

Mr. DESANTIS. The gentlelady yields back. We will now recognize our panel of witnesses. I'm pleased to welcome Dr. George Baker, Professor Emeritus at James Madison University and CEO of BAYCOR; Dr. Peter Vincent Pry, executive director of the Task Force on National and Homeland Security; and Mr. Mike Caruso, Director of Government and Specialty Business Development at ETS–Lindgren. Welcome all.

Pursuant to committee rules, witnesses will be sworn in before they testify. So if you guys can rise an raise your right-hand side.

Do you solemnly swear or affirm that the testimony that you are about to give will be the truth, the whole truth, and nothing but the truth, so help you God?

Let the record reflect that all witnesses answered in the affirmative. Thank you and please be seated.

In order to allow time for discussion, please limit your testimony to 5 minutes and you'll see the blinking lights in front of you. When it hits red, that's when you've hit 5 minutes. Your entire written statement will be made a part of the record. And with that, Dr. Baker, you are up for 5 minutes.

WITNESS STATEMENTS

STATEMENT OF GEORGE BAKER

Mr. BAKER. My thanks to Chairman DeSantis and Chairman Lummis, ranking members and committees members for this opportunity to share my concerns about EMP. My name is George Baker, and I've spent most of my professional career protecting the U.S. military from EMP. At the Defense Threat Reduction Agency, I manage the development of the military standards used to protect the Department of Defense systems. As a retired professor, James Madison University and DOD consultant, I now perform EMP vulnerability assessments of key government facilities.

The congressional EMP Commission on which I served as principal staff made a compelling case for protecting critical infrastructure against nuclear EMP and solar storm geomagnetic disturbances, I will also refer to that as GMD. Among potential disasters, EMP and GMD are particularly challenging because the effects can be continental in scale. EMP and GMD disasters are preventable, that's my main point today, they are preventable. We have the engineering, know-how and tools, what is missing is resolve.

I see three reasons why we are not making progress at present on these threats and I'll address these in the rest of my talk. The first is there are many misconceptions about EMP and GMD threats. I'll look at four of those. The first misconception is that only major nuclear powers, such as Russia and China with high-yield thermonuclear devices could effectively execute an EMP attack. In fact, low yield devices obtained by emerging nuclear powers such as North Korea and Iran can produce catastrophic EMP effects.

Misconception two, that a nuclear EMP attack would burn out every exposed electronic system. In fact, based on government tests, we know that smaller self-contained, self-powered systems such as vehicles, handheld radios, disconnected portable generators are often not affected.

Misconception three, EMP effects on critical infrastructure will be limited to nonsevere, nuisance-type affects. In fact, wide area failure of just a few systems, could cause cascading infrastructure collapse, in highly interconnected networks. One example is the 2003 electric blackout of the northeast was precipitated by a single high-voltage line touching a tree, and then proceeded to cascade to the entire northeast.

So, when you extend this concept to a wide area of failures and infrastructure networks, including the Internet, you can see that EMP is an existential threat that we must take very seriously.

Fourth and final misconception I'll address, that is, to protect all other infrastructure against EMP would cost a large fraction of the U.S. GNP. In fact, protecting the electric grid and communication networks alone would provide substantial benefit and be cost effective.

A recent cost study by the Foundation for Resilient Society shows that significant EMP protection could be achieved for an investment in the range of $10 to $30 billion. The second reason we aren't making progress is the stakeholders are in a state of denial. Concerned about cost makes stakeholders, the government and the private sector reluctant to admit EMP vulnerabilities. Actions to date have been limited and ineffective. An example is the joint effort of the Federal Energy Regulatory Commission, that is, FERC, and the North American Electric Reliability Corporation, that is NERC, to set reliability standards for wide area electromagnetic impacts on the electric grid.

The NERC-developed and FERC-approved standards that we have exclude nuclear EMP, despite the opportunity to protect against both GMD and EMP using the same equipment. NERC standards rely on operational procedures that require no physical protection of the electric grid. The largest measured storms are a factor of 10 higher than their benchmark for protection. A sceptic

might suspect that NERC's main objective was to avert liability rather than to protect the American public.

The third reason we aren't making progress is there is no one in charge. There's no single point of responsibility to develop an implement a national protection plan. When I ask NERC officials about EMP protection, they informed me we don't do EMP, that's DOD's responsibility. The Department of Defense tells me, EMP protection for civilian infrastructure is DHS's responsibility. And then when I talk to DHS, I get answers that the protection should be done by the Department of Energy, since they are the infrastructure's sector-specific agency. So we have EMP and GMD protection as finger-pointing exercises at present.

In closing, I have the following recommendation for future progress, the DOD experience with EMP protection has given us the necessary engineering tools, but what we need is the help of your committee to get government to act. First, we need a designated executive authority. The DHS and DOD both are likely candidates. The first order of business would be a national EMP, GMD protection plan and a set of planning scenarios. Second, let us budget for a national program to check the electric grid, including essential supporting infrastructures used for fuel supply and communication. And third, Congress should recognize that the regulatory apparatus conceived in the Energy Policy Act of 2005 is not working. Establishing a new independent commission, solely focused on electric grid reliability would be very helpful, a commission with the power to issue and enforce regulations on its own similar to the Nuclear Regulatory Commission.

The present FERC/NERC arrangement has proved ineffective. Thank you for this opportunity to present my concerns and recommendations, which are more fully explained in my written testimony and I look forward to your questions.

[The prepared statement of Mr. Baker follows:]

Testimony of George H. Baker
Professor Emeritus, James Madison University
Before the
House Committee on National Security and the
House Subcommittee on the Interior of the House Committee on Oversight and Government Reform

Joint Hearing on "The EMP Threat: The State of Preparedness against the Threat of an Electromagnetic Pulse (EMP) Event"
May 13, 2015

Key Findings from the EMP Commission Report of 2008

The Commission to Assess the threat to the United States from Electromagnetic Pulse, on which I served as principal staff, made a compelling case for protecting critical infrastructure against the nuclear electromagnetic pulse (EMP) and geomagnetic disturbances (GMD) caused by severe solar storms. Their 2008 Critical Infrastructure Report explains EMP effects, consequences, and protection means for critical infrastructure sectors. EMP and GMD are particularly challenging in that they interfere with electrical power and electronic data, control, transmission, and communication systems organic to nearly all critical infrastructures. The affected geography may be continental in scale. EMP and GMD events thus represent a class of high-consequence disasters that is unique in its coverage, ubiquity, and simultaneous system debilitation. Such disasters deserve particular attention with regard to preparedness and recovery since assistance from non-affected regions of the nation could be scarce or nonexistent. The major point I want to make to Congress is that such disasters are preventable. We have the engineering know-how and tools to protect ourselves. What is lacking is resolve.

Brief Tutorial on EMP and GMD Phenomenology

A brief tutorial on EMP and GMD phenomenology will be helpful to the discussion. The nuclear electromagnetic pulse (EMP) results from a nuclear burst high above the jet stream. A similar effect can occur naturally when an intense wave of charged particles from the sun perturbs the earth's magnetic field, causing a solar storm GMD.

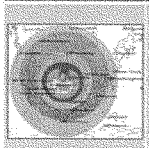
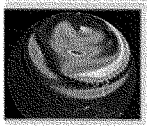
In the case of high altitude nuclear bursts, two main EMP types come into play that I will refer to as the "fast pulse" and the "slow pulse." The fast pulse EMP field, also referred to as E1, is created by gamma ray interaction with stratospheric air molecules. It peaks at tens of kilovolts per meter in a few nanoseconds, and lasts for a few hundred nanoseconds. The broad-band frequency content of E1 (0-1000 megahertz) enables it to couple to electrical and electronic systems in general, regardless of the length of their penetrating cables and antenna lines. Induced currents range into the 1,000s of amperes. Exposed

systems may be upset or permanently damaged.

The "slow pulse" EMP, also referred to as E3, is caused by the distortion of the earth's magnetic field lines due to the expanding nuclear fireball and rising of heated and ionized layers of the ionosphere. The change of the magnetic field at the earth's surface induces currents of hundreds to thousands of amperes in long conducting lines (with lengths of a few kilometers or greater) that damage components of the electric power grid itself as well as powered systems. Long-line communication systems are also affected, including copper as well as fiber-optic lines with repeaters. Transoceanic cables are a prime example of the latter.

Solar storm GMD effects are the result of large excursions in the flux levels of charged particles from the Sun and their interactions with the Earth's magnetic field. The electrojets from these storms, depending on their orientation, generate overvoltages in long-line systems over large regions of the earth's surface affecting electric power and communication transmission networks in a similar fashion to EMP/E3. Note that protecting long-line systems against EMP (E1 and E3) also affords protection against GMD effects. The converse is not true. Protecting electric transmission systems against solar storm GMD/E3 does protect against EMP/E3 –but defending against the fast pulse EMP/E1requires different equipment.

A summary of the nuclear and solar environments of concern is provided in the table below.

	THREAT	Environments	Susceptible Systems
	High Altitude EMP	Fast Pulse E1	Long-line and short-line electrical and electronic systems
		Slow Pulse E3	Long-line network systems incl. electric power grid, terrestrial and undersea comm. lines, pipelines
	Solar Super Storms	Geomagnetic Disturbance	Long-line network systems incl. electric power grid, terrestrial and undersea comm. lines, pipelines

Long-line connected equipment is especially vulnerable to EMP and GMD

Similar to protecting critical infrastructure against any hazard, it will be important to develop risk-based priority approach for the solar GMD and nuclear EMP threats, recognizing that it will be fiscally impracticable to protect everything. Because electromagnetic threat environments are measured in volts per meter, a given system's vulnerability increases with the length of its connecting lines. Because the electric power grid and long-haul communications network (including telephone and Internet) deliver services on long-lines, these infrastructures are the most vulnerable to EMP and GMD. It is ironic that the infrastructures most vulnerable to EMP and GMD are arguably the most critical to society, not only for day-to-day enterprise and life support, but also for recovery were disasters to occur.

Since a simple measure of risk is the multiplicative product of vulnerability and criticality, the electric power and the long-haul telecommunications networks sit at the top of the risk ranking hierarchy. Thus, attention to the electric power grid and long-haul communications infrastructures would bring major benefits to national resiliency. Of these two, the electric power grid is the arguably the most important – all other infrastructures ride on the electric power system. And the grid is the most essential infrastructure for sustaining population life-support services. And the electric power system operation is brittle and binary, and fails fast and hard. Some essential heavy-duty electric power grid components take months to replace – or years if large numbers are damaged. A primary example is high voltage transformers which are known to irreparably fail during major solar storms and are thus likely to fail during an EMP event. Protection of these large transformers will buy valuable time in restoring the grid and the lifeline services it enables. By contrast, communications networks are more malleable due to their technological diversity and the relative ease of component replacement and repair.

DoD has adopted protective priorities using commercial protective equipment

We have much to learn from the Department of Defense (DoD) experience in prioritizing and protecting systems since the 1960s. The DoD has prioritized and has protected selected systems against EMP (and, by similitude to E3, GMD effects). DoD places emphasis on protecting its strategic triad and associated command, control, communications, computer, and intelligence (C^4I) systems.

Although DoD has been successful in protecting its high priority systems dating back to the Minuteman system procurement in the 1960s, our civilian enterprise remain unprotected. In my experience, the lack of progress in protecting civilian infrastructures to EMP and GMD is due to three main factors:

1. There are prevalent misconceptions about EMP and GMD threats and consequences.
2. Stakeholders are reluctant to act.
3. No single organization is the designated executive agent.

I shall address these factors in order.

1. <u>EMP/GMD Misconceptions</u>.

There are many misconceptions about EMP and GMD that are circulating among both technical and policy experts, in press reports, on preparedness websites, and even embedded in technical journals. Because many aspects of the EMP and GMD generation and system interaction physics are non-intuitive, misconceptions are inevitable. Uneasiness about the wide-area, ubiquitous effects of EMP and the diversity of systems affected make it convenient to adopt misconceptions that avoid the need for action. Denying the seriousness of the effect appears perfectly responsible to many stakeholder groups. Misconceptions involving consequence minimization or hyperbole have served to deter action in the past. Downplaying the threats places EMP/GMD preparedness on the back-burner compared to other effects. Exaggeration of the threats causes policy-makers to dismiss arguments, ascribing them to tin foil hat conspiracy theories.

I will address what are perhaps the most harmful misconceptions, viz:

A. Nuclear EMP will burn out every exposed electronic system.

B. Alternatively, EMP/GMD effects will be very limited and only result in "nuisance" effects in critical infrastructure systems.

C. Megaton class weapons are needed to cause any serious EMP effects – low yield, "entry-level" weapons will not cause serious EMP effects.

D. To protect our critical national infrastructure against EMP and GMD would cost a large fraction of the GNP

<u>Misconception A: Nuclear EMP will burn out every exposed electronic system.</u>

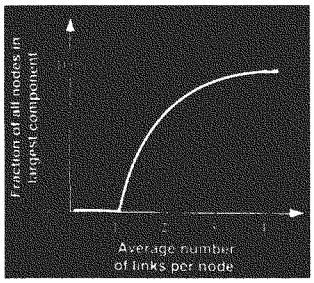
Based on DoD and Congressional EMP Commission's EMP test data bases we know that smaller, self-contained systems that are not connected to long-lines tend not to be affected by EMP fields. Examples of such systems include vehicles, hand-held radios, and disconnected portable generators. If there is an effect on these systems, it is more often temporary upset rather than component burnout.

On the other hand, threat-level EMP testing also reveals that systems connected to long lines are highly vulnerable to component damage, necessitating repair or replacement. 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 the system and the higher the probability of EMP damage. Because of their organic long lines, the electrical power grid network and long-haul landline communication systems are almost certain to experience component damage when exposed to EMP with cascading effects to most other (dependent) infrastructure systems.

Misconception B: EMP effects will be very limited and cause only easily recoverable "nuisance" type effects in critical infrastructure systems.

Although EMP does not affect every system, widespread failure of limited numbers of systems will cause large-scale cascading failures of critical infrastructure systems and system networks because of the interdependencies among the failed subsystems and the interlinked electrical/electronic systems not directly affected by the EMP.



Paul Erdos' "small world" network theory applies to EMP failure analysis.[1] The graph above illustrates that the average fraction of nodes in any network that are connected to any single network node changes suddenly when the average number of links per node exceeds one. For example, a failed node, where the average links per node is 2, can affect ~ 50% of the remaining network nodes.

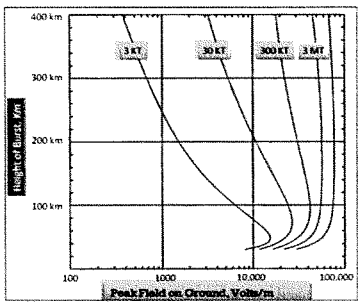
Moreover, for many systems, especially computer controlled machinery and unmanned systems, upset is tantamount to permanent damage – and may cause permanent damage including structural damage in some cases, to systems due to interruption of control. Examples include:

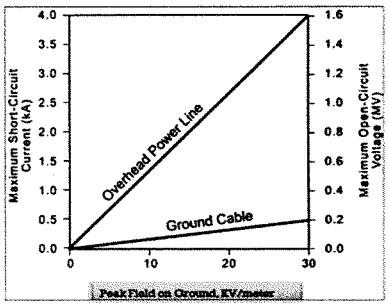
- Upset of generator controls in electric power plants
- Upset of robotic machine process controllers in manufacturing plants
- Lockup (and need for reboot) of long-haul communication repeaters
- Upset of remote pipeline pressure control SCADA system

[1] Duncan Watts, Six Degrees: The Science of the Connected Age, 2004.

Misconception C: Megaton-class nuclear weapons are required to cause serious EMP effects. "Entry-level," kiloton-class weapons will not produce serious effects.

Due to a limiting atmospheric saturation effect in the EMP generation process, low yield weapons produce peak E1 fields of the same order of magnitude as large yield weapons if they are detonated at altitudes in the 50-80 km range. The advantage of high yield weapons is that their field on the ground is attenuated less significantly at larger heights of burst (that expose larger areas of the Earth's surface.





The first graph above illustrates that nominal weapons with yields ranging from 3 kilotons to 3 megatons (a 3 order of magnitude difference in yield), exhibit a range of peak E1 fields on the ground with only a factor of 3 difference, i.e. 15kV/meter vs. 50 kV/meter. Although E3 fields vs. yield and height of burst are not illustrated above, a 30 kiloton nuclear weapon detonated above 100 km can cause magnetic field disturbances as large as solar superstorms, although over smaller regions.

The second graph above indicates that megavolt levels and kiloampere-level currents are induced in long overhead lines by E1 from kiloton-class weapons, such as those that might be produced by an emerging nuclear power.

Misconception D: to protect our critical national infrastructure against EMP and GMD would cost a large fraction of the U.S. Gross National Product.

Among the critical infrastructure sectors, EMP risk is highest for electric power grid and telecommunication grids – attention to these infrastructures alone would bring major benefits to national resiliency and enhance deterrent effects. These infrastructures are the most vulnerable due to their organic long lines. And they are also the most critical to the operation and recovery of the other critical infrastructure sectors. As mentioned

previously, if we have to pick one infrastructure to protect, the top choice would be the electric power grid.

The Foundation for Resilient Societies, a non-profit organization on which I serve as a member of the Board of Directors, has developed a comprehensive cost estimate for grid protection that includes costs for protecting the grid and the portions of other sectors required for grid operation, viz. fuel supply and communication. Resiliency of the electric grid depends upon concurrent protection of key telecommunications, Class 1 railroad systems that transport coal to generation plants, and interstate natural gas pipeline systems. The combined costs, summarized here, are in the range of $30 Billion.

The costs to protect roughly the transmission and distribution system and half of the U.S. generation capacity are provided in the table below:

Resilient Societies Cost Projections

Electric Generation Plants	$23,0000M
Electricity Transmission & Distribution	$2,300M
Electric Grid Control Centers	$1,390.M
Telecommunications	$1,480M
Natural Gas System	$640M
Railroads	$1,380M
Blackstart Plant Resiliency	$80M
	$30,270M

Using the $30,270 bottom line EMP and GMD protection cost estimate and a levelized annual revenue requirement of 20% ($6B), assuming there are ~150 million rate payers in the United States, the estimated annual cost per rate payer would be $3.30 per month.

There are strong arguments for protecting selected subsets of the grid. For example, a top priority to ensure situational awareness following a GMD or EMP event would be to protect major grid control centers. Estimates to protect these are in the $1.4 billion ballpark. If a Phase 1 EMP/GMD program operated in 2016-2020 at a five year cost of $1.4 billion, or $280 million per year, and all the extra costs were passed through to retail customers, the extra cost would be approximately $0.16 per electric customer per month.

We also might put priority on ensuring the survivability of major grid components that would take months to replace –or years if large numbers suffer damage. A primary example would be high voltage transformers which are known to irreparably fail during major solar storms and are thus also vulnerable to failure during an EMP event. Protection of these large transformers would save valuable time in restoring the grid and the life-support services it enables. The unit cost for HV transformer protection is estimated to be

$350,000. The total number of susceptible units range from 300 – 3000 (further assessment is required to establish an exact number.) Doing the math, the protected cost for protecting 3000 of these longest replacement lead-time components of the grid is $ 1 billion – a small fraction of the value of losses (Lloyds of London estimates are in the trillions of dollars[2] for GMD alone) and long-term recovery costs should they fail.

2. Stakeholder Reluctance.

Concern about costs and liabilities makes stakeholders in government and the private sector reluctant to admit vulnerabilities. A major impediment to action on protecting the grid against GMD and EMP effects has been that government and industry are (understandably) swayed by the familiar, the convenient, and the bottom line. Like it or not, familiarity and profitability are the touchstones of acceptability – strategic advantage goes to the convenient. Thus, the tendency exists to downplay the likelihood of EMP and GMD and their associated consequences. The prevalent misconceptions (factor 1) have also contributed to stakeholders' ability to downplay the seriousness of EMP and GMD effects to avoid action.

In cases where stakeholders have decided to take action to improve infrastructure survivability, the actions have been limited and ineffective. A primary case in point is the NERC effort to set reliability standards for wide-area electromagnetic effects. Responding to FERC's inquiries for protection standards, the NERC formed a GMD task force. When several task force participants asked why EMP could not be part of the task force deliberations, NERC leadership explained that EMP was a national defense concern and therefore not their responsibility – rather that DoD should take the lead.

The standards ultimately developed by NERC include a set of operational procedures requiring no physical protection of the electric grid and a scientifically-flawed benchmark GMD threat description that enables most U.S. utilities to avert installing physical protection based on their own paper modeling studies. The benchmark GMD threat description is based on solar storm statistics over the last 25 years during which there were no "Carrington Class" 100-year solar superstorms. The Carrington-class storm GMD levels are an order of magnitude higher than the largest storms in the NERC 25 year data window. NERC's benchmark event is admissible only if we assume that all eleven-year solar cycles are the same, an assumption known to be incorrect. A skeptic might suspect that the NERC standard's main objective was to avert liability rather than protect the public from serious GMD consequences.

---

[2] Space Weather: It's Impact on Earth and Implications for Business, Lloyds of London, 2010. In this report Lloyds advocates development of robust systems designed to operate through space weather events.

The outcome of the NERC operational procedures standard, now approved by FERC, is that the public will not be protected from EMP and the industry will deal with GMD effects using operational work-around procedures such as shedding load and spinning up reserve generation capacity.

The operational procedure-based solutions that have been offered by NERC in their recently adopted EOP-010-01-1 standard are ineffective for a number of reasons. A non-exhaustive list of ten pitfalls accompanying reliance on operational procedures to protect the electric power grid follows.

1. GMD operating procedures are based on the premise that operators can and will prevent large-scale grid collapse by shedding load. Due to insurance rules, grid operators will be reluctant to shed load to customers, even though load-shedding procedures reduce the probability of grid collapse and damage to EHV transformers. Utility companies know that if customer electric power is lost due to geomagnetic disturbance (GMD), they will not be liable for losses; but if customer power is lost due to intentional human action to de-energize the grid or portions of it, power companies can be held liable. (Reference the Lloyds of London report on GMD effects and liabilities and statements by insurance company representatives at 2012 Electric Infrastructure Security Summit at UK Parliament).

2. The 15-45 minute warning time earlier provided by the Advanced Composition Explorer (ACE) satellite and now supported by the Deep Space Climate Observatory (DSCOVR) successor will be inadequate for grid operators to confer while executing required operational procedures. Participants in the 2011 National Defense University-Johns Hopkins University GMD response exercise indicated that they would be hard-pressed even to get all the players to the table within such a short time interval. And, once hit, the grid would fail quickly. We note that, in 1989, during a moderate solar storm GMD, the electric power grid of the entire Province of Quebec went dark in 92 seconds. The August 2003 Northeast Blackout evolved much more slowly (1:31pm – 4:10pm) with much more time available to take action. Nonetheless, even with a span of hours available, power companies were unable to react fast enough to prevent grid collapse.

3. Grid operators will not have adequate information on the state of the grid to implement correct operational procedures. Because most of the grid is not monitored for Geomagnetically Induced Currents (GIC), operators will be "flying blind" with respect to the state of the grid. Operators will not know which portions need remedial action and what actions will be optimal. Information gaps will exist as in August 2003 – where operators were unaware of the initiating tree contact. Sensors needed to monitor GMD/EMP stressors on critical grid components were not required by NERC standards and have not

been installed. And this lack of visibility has led and will lead to errors in executing operational procedures.

4. There is no control center with large enough visibility to control operational procedure response on a national scale. Lack of information on neighboring interconnections impairs proper procedural response. A national control/coordination center does not exist. And in the Eastern Interconnection, there is no single authority over the nine American regional Reliability Coordinators. Because the geographic coverage of solar storm GMD and nuclear EMP can be continental in scale, super-regional control visibility and authority are necessary. At this point, only the federal government, using Presidential authority, can fulfill this role.

5. Operational procedures have not been adequate to address the much simpler causes of previous large-scale blackouts. For instance, operational procedures proved ineffective in preventing the 2003 Northeast blackout that was precipitated by a single failure point – tree contact with a transmission line. Recent grid models indicate that GMD and EMP will cause hundreds to thousands of failure points. The complexity and rapidity of grid failure during a Carrington-class event will overwhelm the ability of electric utilities to respond and to prevent grid failure using any suite of operational procedures, no matter how well-conceived and practiced. During Hurricane Sandy, grid physical damage outstripped the effectiveness of procedural protection efforts. Physical damage to grid components will be a factor in GMD/EMP events as well.

6. Unforeseen grid equipment malfunctions have greatly impaired grid operators' ability to respond during major blackouts in the past. Operational procedures during the 2003 Northeast blackout were greatly impaired by computer control system malfunctions and software problems. Critical grid state monitoring, logging and alarm equipment failed. The control area's SCADA and emergency management systems malfunctioned. The shut-down of hundreds of generators over multiple states was unanticipated as was the failure of tens of transmission lines. Confusion and inoperative control systems led to many frantic phone calls. As these events, show, any early failure of major grid components caused by the GMD or EMP environment will impede implementation of subsequent operational procedures.

7. EMP and GMD will affect the communication systems necessary for coordination of operational procedures. Long-line internet and telecommunications networks will experience large overvoltages from GMD and EMP E1/E3 environments, likely causing their debilitation. GMD and EMP also impede signal propagation of HF/VHF/UHF radio systems and GPS systems. Thus grid communication and control systems necessary to execute operational procedures cannot be relied on – just when they will be needed the most.

8. It is not possible to anticipate all grid failure point combinations and time sequences during GMD/EMP events in order to adequately plan, exercise, and test GMD/EMP operational procedures. Normal grid failures are not indicative of GMD/EMP failures. Operators are familiar with commonly occurring single equipment failures but when multiple points fail near simultaneously under GMD/EMP stress, and the failures interact and cascade, operators will have difficulty understanding and responding to prevent further damage.

In most complex human-machine systems, the interactions literally cannot be seen. Prof. Charles Perrow of Yale defines 'normal accidents' in complex infrastructure systems as involving system interactions that are not only unexpected, but are incomprehensible for some critical period of time. For example, 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.

9. In the Eastern Interconnection, Regional Transmission Organizations (RTOs) and Independent System Operators (ISO's) don't have cross-jurisdictional authority to enforce shutdown of neighboring grids, sometimes required to avoid large scale blackouts, as in the August 2003 Northeast Blackout. There is no overall supervisor for the Eastern Interconnection. During the 2003 Northeast blackout, First Energy was asked to shed load by its neighboring grid operators but First Energy declined. According to the NERC after-action report, load shedding would have prevented the ensuing Northeast blackout.

10. Draft NERC GMD operational procedures recently approved by FERC (Order No. 797, June 2014) are not comprehensive and not specific. The plans generator operators and load balancing authorities from mitigation responsibilities. The NERC operational procedures also exempt portions of the grid operating below 200kV. In the August 2003 blackout, failure of 125 kV lines played a major role in the collapse of the Northeast grid.

The GMD operational procedures and solar storm benchmark event approved by FERC are ineffective and allow the electric power industry to continue with no significant upgrades to their physical assets, leaving the grid vulnerable to 100 year solar superstorms and EMP. It is worth noting that while GMD fields are more intense at northern latitudes, E3 fields increase at more southerly latitudes relative to the locus of a high altitude EMP event. Utilities that require no protection against GMD because of their southerly latitude under the newly operative standard would be experience higher E3 fields in the event of an EMP event than their northerly counterparts. The bifurcated "stove-pipe" threat approach being pursued to protect the electric power grid is cost- and outcome-ineffective. We need to develop a unified, all-threat approach to this challenge which leads to the third and final impediment to progress:

3. There is no one in charge.

To a major extent, the lack of progress in protecting our most critical infrastructure to EMP and GMD is that the responsibility is distributed. There is no single point of responsibility to develop and implement a national protection plan. Nobody is in charge. When I asked the North American Electrical Reliability Corporation about EMP protection, they informed me, "we don't do EMP, that's a Department of Defense problem." The Department of Defense tells me, "EMP protection of the civilian infrastructure is a DHS responsibility." DHS explained to me that the responsibility for the electric power grid protection is within DOE since they are the designated Sector Specific Agency (SSA) for the energy infrastructure.

EMP protection has become a finger pointing, "ring around the rosey," duck-and-cover game. Our bureaucracy has enabled gaps for addressing the difficult problems of EMP and GMD, resulting in no substantive action to protect the nation. We have the classic Washington problem of issues that span departments or fall between departments, which we're all very familiar with, but then we add to that the involvement of the private sector, without central leadership, we're foundering. Because these catastrophes can be continental in scale with everyone in trouble, and there's nobody left to help, the ultimate solution, by default, has fallen to the state and local levels. States are entitled to protect the safety, reliability and adequacy" of their electric grids, but most states expect the federal government to provide leadership in protecting the bulk power system. Local level preparedness is crucial, but we still need federal top down guidance to achieve a uniform, coordinated approach to the problem – to be able to triage, to standardize protection methods across the states and localities. We know, and I've stressed, that we can't protect everything. Uniform guidance is needed to determine what needs to be protected and assign responsibilities. Local jurisdictions need top-level guidance and information to understand what to do.

The current state of EMP protection is random, disoriented and uncoordinated. As we go forward, I suggest that Congress establish a responsible party or agency to be the central whip for EMP preparedness. That would change the landscape materially and make progress possible.

Recommendations for Future Progress.

We must come to grips as a nation with the EMP/GMD preparedness challenges. The consequences of these threats are preventable. The good news is that the engineering

tools are available to protect a meaningful set of high-priority infrastructures.[3] There are a number of initiatives that would greatly aid in this endeavor.

First, a designated national executive agency and director is needed. DHS and DoD are likely candidates. Of these, DoD has the most experience. The first order of business should be a national EMP/GMD protection plan and a set of national planning scenarios.

Second, let us begin a national program to protect the electric power grid, including essential supporting infrastructures used for fuel supply and communication.

Third, Congress should address problems inherent in the regulation of electric reliability as conceived in the Energy Policy Act of 2005. Establishing a new independent commission solely focused on electric grid reliability would be helpful – a commission with the power to issue and enforce regulations, similar to the Nuclear Regulatory Commission. The present FERC-NERC arrangement has proven ineffective with respect to EMP/GMD preparedness.

Thank you for the opportunity to share my perspective on EMP and GMD issues and solutions.

Respectfully Submitted,

George H. Baker
Professor Emeritus
James Madison University

[3] The Electric Infrastructure Security Council has recently published an Electric Infrastructure Protection Handbook and Mil-STD-188-125 provides guidance for protecting communication and data systems.

Mr. DESANTIS. Thank you, Dr. Baker.

The chair now recognizes Dr. Pry for 5 minutes, you are up.

STATEMENT OF PETER VINCENT PRY

Mr. PRY. Thank you for the opportunity to address the subcommittees today. First, what I think we must understand about the threat is that it is not merely theoretical, it is a real threat. In the military doctrines of Russia, China, North Korea and Iran, they plan to make a nuclear EMP attack against the United States. We have seen North Korea and Iran exercise this, including by launching ballistic missiles off of a freighter at sea, which would enable the possibility of an anonymous EMP attack. During the nuclear crisis we had with North Korea in 2013, it was the worst nuclear crisis we ever had with Kim Jong Un was threatening to make nuclear missile strikes against the United States in the aftermath of their third illegal nuclear test.

In the midst of that crisis North Korea orbited a satellite over the south pole that passed over the territory of the United States on the optimum trajectory and altitude to both evade our national missile defenses, and, had that been a nuclear warhead, to place an EMP field over all 48 contiguous United States that would have had catastrophic consequences. That was the KSM 3 satellite; that satellite stills passes over us, it's sill in orbit and passes over us with regularity.

Another thing that must be understood is that EMP is part of a—a larger part of their military doctrine that they consider a revolution in military affairs. That, basically, is a combined arms operation with cyber attacks, physical sabotage, nonnuclear EMP weapons, and nuclear EMP weapons is the most decisive instrument all used together and coordinated in a formula new Blitzkrieg, except one that's waged in cyberspace to basically bring a civilization down to its knees so that a failed state like an Iran or North Korea could theoretically defeat and destroy a highly advanced society like our own.

This would be unprecedented in history where you would have a situation where a state like Iran or North Korea or even a sub national actor like a terrorist group if they could get hold of that one nuclear bomb and do it in combination with cyber attacks and physical sabotage to crash our critical infrastructures, especially the electric grid and basically destroy our civilization. But they write about it; they exercise it; they are serious about it. And we actually see this being practiced in real life in some countries back in June of last year while ISIS was sweeping over northern Iraq, al Qaeda and the Arabian Peninsula blacked out the entire electric grid in the state of Yemen, put 18 cities and 24 million people into the dark. That is the first time in history that a terrorist group has blacked out a whole country. And it so destabilized Yemen that look what happened to them. They have gone from being a U.S. ally, so now we have lost one of our most important allies in the Middle East already to this kind of an attack.

This year, in January 25 of this year, a terrorist group blacked out 80 percent of the grid in Turkey. We don't know what they are up to in doing that—excuse me, in Pakistan, but Pakistan is a nuclear weapons State. So the idea that 80 percent of the grid could

be blocked out in Pakistan for purposes unknown is extremely disturbing.

Is this a precursor to try to get their hands on nuclear weapons in Pakistan? About a week before the Washington blackout happened, Turkey was put—80 percent of Turkey was put into blackout by a cyber attack by Iran. These were not EMP attacks, but they are experiments with parts of this doctrine that they have that would combine all these things and we have seen in the case of North Korea and Iran experiments with the nuclear EMP option as well.

Now, so the threat is real. As George Baker has testified, however, there is really no excuse for us to be vulnerable to this. We know how to fix the problem, and one of the things the EMP Commission recommended was, if you can protect against the worst threat, which is the nuclear EMP attack, if you can protect against that, it will mitigate all the others: Cyber attacks, physical sabotage, nonnuclear EMP weapons and GMD as well. So we know how to fix the problem.

What to do? I endorse everything that Dr. Baker said. We need to pass the Critical Infrastructure Protection Act. The importance of having a national planning scenario focused on EMP cannot be understated.

Right now, despite what DHS may be telling you, if it is not in the national planning scenarios, the threat doesn't exist for State and local emergency planners, or for Federal emergency planners, too. People who want do something about this threat at the State level when they apply for funding, for example, from DHS, can't get it because EMP is not among the national planning scenarios. So that would put it on the radar screen for Federal, State and local emergency planners and would be an enormous step forward toward solving the problem.

Next, we need to bring back the congressional EMP Commission, which is actually under consideration right now in the Defense Authorization bill being negotiated with the Senate. The greatest progress we made in this country was when the EMP Commission was around and, you know, with the absence of the Commission, well we have seen that no progress has been made. If we can bring back the EMP Commission, I expect that that would reintroduce, we would have a voice in the governmental level part of Congress that could aggressively promote EMP preparedness, and that is what we need to do.

And last, the NERC/FERC relationship, I completely agree with Dr. Baker. It's extremely dysfunctional, it doesn't work. It needs to be reformed. I'm not sure that you can actually reform those institutions. I would actually advocate abolishing both FERC and NERC and starting with something else, a different kind of institution, something similar to the Nuclear Regulatory Commission that has real regulatory power, and that understands that its stakeholder, its customer is not the electric power industry first, but it's the American people first. And the responsibility is first not to the profits of the utilities, but it's to America's national security. Thank you for hearing me out.

[The prepared statement of Mr. Pry follows:]

DR. PETER VINCENT PRY
STATEMENT FOR THE RECORD
JOINT HEARING BEFORE THE
SUBCOMMITTEE ON NATIONAL SECURITY
SUBCOMMITTEE ON THE INTERIOR
HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
Rayburn HOB Room 2247
May 13, 2015

The EMP Threat: The State of Preparedness Against the Threat of a Electromagnetic Pulse (EMP) Event

Natural EMP from a geomagnetic super-storm, like the 1859 Carrington Event or 1921 Railroad Storm, or nuclear EMP attack from terrorists or rogue states, as apparently practiced by North Korea during the nuclear crisis of 2013, are both existential threats that could kill up to 9 of 10 Americans through starvation, disease, and societal collapse. A natural EMP catastrophe or nuclear EMP attack could blackout the national electric grid for months or years and collapse all the other critical infrastructures--communications, transportation, banking and finance, food and water--necessary to sustain modern society and the lives of 310 million Americans.

Most the general public and most State governments are unaware of the EMP threat and that:

- **Political gridlock in Washington has prevented the Federal government from implementing any of the several cost-effective plans for protecting the national electric grid;**
- **Most State governments are unaware that they can protect that portion of the grid within their State and so protect their citizens from the catastrophic consequences of a national blackout;**
- **The electric grid is the keystone critical infrastructure necessary to recover all other critical infrastructures;**
- **Protection of the grid from EMP, which is the worst threat, will also enhance overall grid security against all other threats, including cyber attack, sabotage, and severe weather.**

All Hazards Strategy--EMP Protection Key

The Congressional EMP Commission warned that an "all hazards" strategy should be pursued to protect the electric grid and other critical infrastructures. An "all hazards" strategy means trying to find common solutions that protect against more than one threat--ideally against all threats.

The "all hazards" strategy is the most practical and most cost-effective solution to protecting the electric grid and other critical infrastructures. Electric grid operation and vulnerability is critically dependent upon two key technologies--Extra-High Voltage (EHV) transformers and Supervisory Control and Data Acquisition Systems (SCADAS).

EHV Transformers
EHV transformers are the technological foundation of our modern electronic civilization as they make it possible to transmit electric power over great distances. An EHV transformer typically is as large as a house, weighs hundreds of tons, costs millions of dollars, and cannot be mass produced but must be custom-made by hand. Making a single EHV transformer takes about 18 months. Annual worldwide production of EHV transformers is about 200 per year.

Unfortunately, although Nikolai Tesla invented the EHV transformer and the electric grid in the U.S., EHV transformers are no longer manufactured in the United States. Because of their great size and cost, U.S. electric utilities have very few spare EHV transformers. The U.S. must import EHV transformers made in Germany or South Korea, the only two nations in the world that make them for export.

An event that damages hundreds--or even as few as 9--of the 2,000 EHV transformers in the United States could plunge the nation into a protracted blackout lasting months or even years.

SCADAS
SCADAS are basically small computers that run the electric grid and all the critical infrastructures. For example, SCADAS regulate the flow of electric current through EHV transformers, the flow of natural gas or of water through pipelines, the flow of data through communications and financial systems, and operate everything from traffic control lights to the refrigerators in regional food warehouses.

SCADAS are ubiquitous in the civilian critical infrastructures, number in the millions, and are as indispensable as EHV transformers to running our modern electronic civilization.

An event that damages large numbers of SCADAS would put that civilization at risk.

Nuclear EMP--The Worst Threat
High-altitude nuclear EMP attack is the greatest single threat that could be posed to EHV transformers, SCADAS and other components of the national electric grid and other critical infrastructures. Nuclear EMP includes a high-frequency electromagnetic shockwave called E1 EMP that can potentially damage or destroy virtually any electronic system having a dimension of 18 inches or greater.

E1 EMP is unique to nuclear weapons.

Consequently, a high-altitude nuclear EMP event could cause broad damage of electronics and critical infrastructures across continental North America, while also causing deep damage to industrial and personal property, including to automobiles and personal computers.

Nuclear EMP can also produce E2 EMP, comparable to lightning.

In contrast, natural EMP from a geomagnetic super-storm generates no E1 EMP, only E3 EMP (technically called magneto-hydrodynamic EMP, or E3 for short). E3 EMP has such long wavelengths that it requires a large "antennae" of about 1 kilometer or more in length, such as

power lines, telephone lines, pipelines, and railroad tracks. E3 EMP cannot enter directly relatively small targets such as automobiles or personal computers.

However, while a geomagnetic super-storm would not directly damage relatively small electronic systems, a protracted nationwide blackout resulting from such a storm would within days stop everything. Personal computers cannot run for long on batteries, nor can automobiles run without gasoline.

Nuclear EMP can also produce E3 EMP comparable to or greater than a geomagnetic super-storm. Even a relatively low-yield nuclear weapon, like the 10-kiloton Hiroshima bomb, can generate an E3 EMP field powerful enough to damage EHV transformers.

The Congressional EMP Commission recommended protecting the electric grid and other critical infrastructures against nuclear EMP as the best basis for an "all hazards" strategy. Nuclear EMP may not be as likely as other threats, but it is by far the worst, the most severe, threat.

The EMP Commission found that if the electric grid can be protected and quickly recovered from nuclear EMP, the other critical infrastructures can also be recovered, with good planning, quickly enough to prevent mass starvation and restore society to normalcy. If EHV transformers, SCADAS and other critical components are protected from the worst threat--nuclear EMP--then they will survive, or damage will be greatly mitigated, from all lesser threats, including natural EMP from geomagnetic storms, severe weather, sabotage, and cyber attack.

The New "Lightning War"

The "all hazards" strategy recommended by the EMP Commission is not only the most cost-effective strategy--it is a necessary strategy. U.S. emergency planners tend to think of EMP, cyber, sabotage, severe weather, and geo-storms in isolation, as unrelated threats

However, potential foreign adversaries in their military doctrines and actual military operations appear to be planning an offensive "all hazards" strategy that would throw at the U.S. electric grid and civilian critical infrastructures--every possible threat simultaneously

Iran, North Korea, China and Russia appear to be perfecting what Moscow calls a "Revolution in Military Affairs" that is potentially more decisive than Nazi Germany's Blitzkrieg ("Lightning War") strategy that nearly conquered the western democracies during World War II. The New Lightning War would attack the electric grid and other critical infrastructures--the technological and societal Achilles Heel of electronic civilization--with coordinated employment of cyber, sabotage, and EMP attacks, possibly timed to leverage severe space or terrestrial weather.

While gridlock in Washington has prevented the Federal Government from protecting the national electric power infrastructure, threats to the grid--and to the survival of the American people--from EMP and other hazards are looming ever larger. Grid vulnerability to EMP and other threats is now a clear and present danger.

Geomagnetic Storms

Natural EMP from geomagnetic storms, caused when a coronal mass ejection from the Sun collides with the Earth's magnetosphere, poses a significant threat to the electric grid and the critical infrastructures, that all depend directly or indirectly upon electricity. Normal geomagnetic storms occur every year causing problems with communications and electric grids for nations located at high northern latitudes, such as Norway, Sweden, Finland and Canada.

For example, the 1989 Hydro-Quebec Storm blacked-out the eastern half of Canada in 92 seconds, melted an EHV transformer at the Salem, New Jersey nuclear power plant, and caused billions of dollars in economic losses.

In 1921 a geomagnetic storm ten times more powerful, the Railroad Storm, afflicted the whole of North America. It did not have catastrophic consequences because electrification of the U.S. and Canada was still in its infancy. The National Academy of Sciences estimates that if the 1921 Railroad Storm recurs today, it would cause a catastrophic nationwide blackout lasting 4-10 years and costing trillions of dollars.

The Carrington Event

The most powerful geomagnetic storm ever recorded is the 1859 Carrington Event, estimated to be ten times more powerful than the 1921 Railroad Storm and classed as a geomagnetic super-storm.

Natural EMP from the Carrington Event penetrated miles deep into the Atlantic Ocean and destroyed the just laid intercontinental telegraph cable. The Carrington Event was a worldwide phenomenon, causing fires in telegraph stations and forest fires from telegraph lines bursting into flames on several continents. Fortunately, in the horse and buggy days of 1859, civilization did not depend upon electrical systems.

Recurrence of a Carrington Event today would collapse electric grids and critical infrastructures all over the planet, putting at risk billions of lives. Scientists estimate that geomagnetic super-storms occur about every 100-150 years. The Earth is probably overdue to encounter another Carrington Event.

NASA warns that on July 22, 2012, a powerful solar flare narrowly missed the Earth that would have generated a geomagnetic super-storm, like the 1859 Carrington Event, and collapsed electric grids and life sustaining critical infrastructures worldwide.

The National Intelligence Council (NIC), that speaks for the entire U.S. Intelligence Community, published a major unclassified report in December 2012 *Global Trends 2030* that warns a geomagnetic super-storm, like recurrence of the 1859 Carrington Event, is one of only eight "Black Swans" that could by or before 2030 change the course of global civilization. The NIC concurs with the consensus view that another Carrington Event could recur at any time, possibly before 2030, and that, if it did, electric grids and critical infrastructures that support modern civilization could collapse worldwide.

NASA estimates that the likelihood of a geomagnetic super-storm is 12 percent per decade. This virtually guarantees that Earth will experience a natural EMP catastrophe in our lifetimes or that of our children.

NERC "Operational Procedures" Non-Solution

The North American Electric Reliability Corporation (NERC), the lobby for the electric power industry that is also supposed to set industry standards for grid security, claims it can protect the grid from geomagnetic super-storms by "operational procedures." Operational procedures would rely on satellite early warning of an impending Carrington Event to allow grid operators to shift around electric loads, perhaps deliberately brownout or blackout part or all of the grid in order to save it. NERC estimates operational procedures would cost the electric utilities almost nothing, about $200,000 dollars annually.

Critics rightly argue that NERC's proposed operational procedures is a non-solution designed as an excuse to avoid the expense of the only real solution--physically hardening the electric grid to withstand EMP.

The ACE satellite is aged and sometimes gives false warnings that are not a reliable basis for implementing operational procedures. While coronal mass ejections can be seen approaching Earth typically about three days before impact, the Carrington Event reached Earth in only 11 hours, and the Ace satellite cannot warn whether a geo-storm will hit the Earth until merely 20-30 minutes before impact.

Most recently, on September 19-20, 2014, the National Oceanic and Atmospheric Administration and NERC demonstrated again that they are unable to ascertain until shortly before impact whether a coronal mass ejection will cause a threatening geomagnetic storm on Earth.

There is no command and control system for coordinating operational procedures among the 3,000 independent electric utilities in the United States. Operational procedures routinely fail to prevent blackouts from normal terrestrial weather, like snowstorms and hurricanes. There is no credible basis for thinking that operational procedures alone would be able to cope with a geomagnetic super-storm--a threat unprecedented in the experience of NERC and the electric power industry.

NERC has not helped its case by being caught red handed peddling "junk science" that grossly underestimates the threat from another Carrington Event.

States Should EMP Harden Their Grids

NERC rejects the recommendation of the Congressional EMP Commission to physically protect the national electric grid from nuclear EMP attack by installing blocking devices, surge arrestors, faraday cages and other proven technologies. These measures would also protect the grid from the worst natural EMP from a geomagnetic super-storm like another Carrington Event. The estimated one time cost--$2 billion dollars--is what the United States gives away every year in foreign aid to Pakistan.

Yet Washington remains gridlocked between lobbying by NERC and the wealthy electric power industry on the one hand, and the recommendations of the Congressional EMP Commission and other independent scientific and strategic experts on the other hand. The States should not wait for Washington to act, but should act now to protect themselves.

Catastrophe from a geomagnetic super-storm may well happen sooner rather than later--and perhaps in combination with a nuclear EMP attack.

Paul Stockton, President Obama's former Assistant Secretary of Defense for Homeland Defense, on June 30, 2014, at the Electric Infrastructure Security Summit in London, warned an international audience that an adversary might coordinate nuclear EMP attack with an impending or ongoing geomagnetic storm to confuse the victim and maximize damage. Stockton notes that, historically, generals have often coordinated their military operations with the weather. For example, during World War II, General Dwight Eisenhower deliberately launched the D-Day invasion following a storm in the English Channel, correctly calculating that this daring act would surprise Nazi Germany.

Future military planners of the New Lightning War may well coordinate a nuclear EMP attack and other operations aimed at the electric grid and critical infrastructures with the ultimate space weather threat--a geomagnetic storm.

Severe Weather

Hurricanes, snow storms, heat waves and other severe weather poses an increasing threat to the increasingly overtaxed, aged and fragile national electric grid. So far, the largest and most protracted blackouts in the United States have been caused by severe weather.

For example, Hurricane Katrina (August 29, 2005), the worst natural disaster in U.S. history, blacked out New Orleans and much of Louisiana, the blackout seriously impeding rescue and recovery efforts. Lawlessness swept the city. Electric power was not restored to parts of New Orleans for months, making some neighborhoods a criminal no man's land too dangerous to live in. New Orleans has still not fully recovered its pre-Katrina population. Economic losses to the Gulf States region totaled $108 billion dollars.

Hurricane Sandy on October 29, 2012, caused blackouts in parts of New York and New Jersey that in some places lasted weeks. Again, as in Katrina, the blackout gave rise to lawlessness and seriously impeded rescue and recovery. Thousands were rendered homeless in whole or in part because of the protracted blackout in some neighborhoods. Partial and temporary blackouts were experienced in 24 States. Total economic losses were $68 billion dollars.

A heat-wave on August 14, 2003, caused a power line to sag into a tree branch, which seemingly minor incident began a series of cascading failures that resulted in the Great Northeast Blackout of 2003. Some 50 million Americans were without electric power--including New York City. Although the grid largely recovered after a day, disruption of the nation's financial capital was costly, resulting in estimated economic losses of about $6 billion dollars.

On September 18, 2014, a heat wave caused rolling brownouts and blackouts in northern California so severe that some radio commentators speculated that a terrorist attack on the grid might be underway.

NERC and Electric Utilities Underperform

Ironically, about one week earlier, on September 8-10, 2014, there was a security conference on threats to the national electric grid meeting in San Francisco. There executives from the electric power industry credited themselves with building robust resilience into the electric power grid. They even congratulated themselves and their industry with exemplary performance coping with and recovering from blackouts caused by hurricanes and other natural disasters.

The thousands of Americans left homeless due to Hurricanes Katrina and Sandy, the hundreds of businesses lost or impoverished in New Orleans and New York City, would no doubt disagree.

The U.S. Government Accountability Office (GAO), if it had jurisdiction to grade electric grid reliability during hurricanes, would almost certainly give the utilities a failing grade. Ever since Hurricane Andrew in 1992, the U.S. GAO has found serious fault with efforts by the Federal Emergency Management Agency, the Department of Homeland Security, and the Department of Defense to rescue and recover the American people from every major hurricane. Blackout of the electric grid, of course, seriously impedes the capability of FEMA, DHS, and DOD to do anything.

Since the utilities regulate themselves through the North American Electric Reliability Corporation, their uncritical view of their own performance reinforces a "do nothing" attitude in the electric power industry.

For example, after the Great Northeast Blackout of 2003, it took NERC a decade to propose a new "vegetation management plan" to protect the national grid from tree branches. NERC has been even more resistant and slow to respond to other much more serious threats, including cyber attack, sabotage, and natural EMP from geomagnetic storms.

As noted earlier, NERC flatly rejects responsibility to protect the grid from nuclear EMP attack.

New York and Massachusetts Protect Their Grids

New York Governor Andrew Cuomo and Massachusetts Governor Deval Patrick would not agree that NERC's performance during Hurricane Sandy was exemplary. Under the leadership of Governor Patrick, Massachusetts is spending $500 million to upgrade the security of its electric grid from severe weather. New York is spending a billion dollars to protect its grid from severe weather.

Unfortunately, both States are probably spending a lot more than they have to by focusing on severe weather, instead of an "all hazards" strategy to protect their electric grids.

The biggest impediment to recovering an electric grid from hurricanes is not fallen electric poles and downed power lines. When part of the grid physically collapses, an overvoltage can result that can damage all kinds of transformers, including EHV transformers, SCADAS and other vital

grid components. Video footage shown on national television during Hurricane Sandy showed spectacular explosions and fires erupting from transformers and other grid vital components caused by overvoltage.

If the grid is hardened to survive a nuclear EMP attack by installation of surge arrestors, it would easily survive overvoltage induced by hurricanes and other severe weather. This would cost a lot less than burying power lines underground and other measures being undertaken by New York and Massachusetts to fortify their grids against hurricanes--all of which will be futile if transformers and SCADAS are not protected against overvoltage.

According to a senior executive of New York's Consolidated Edison, briefing at the Electric Infrastructure Security Summit in London on July 1, 2014--Con Ed is taking some modest steps to protect part of the New York electric grid from nuclear EMP attack. This good news has not been reported anywhere in the press.

I asked the Con Ed executive why New York is silent about beginning to protect its grid from nuclear EMP? Loudly advertising this prudent step could have a deterrent effect on potential adversaries planning an EMP attack.

The Con Ed executive could offer no explanation.

New York City because of its symbolism as the financial and cultural capitol of the Free World, and perhaps because of its large Jewish population, has been the repeated target of terrorist attacks with weapons of mass destruction. A nuclear EMP attack centered over New York City, the warhead detonated at an altitude of 30 kilometers, would cover all the northeastern United States with an EMP field, including Massachusetts.

A practitioner of the New Lightning War may be more likely to exploit a hurricane, blizzard, or heat wave than a geomagnetic storm, when launching a coordinated cyber, sabotage, and EMP attack. Terrestrial bad weather is more commonplace than bad space weather.

New York and Massachusetts have both been frontline States in the war on terrorism. Nuclear EMP attack could potentially put in the frontlines--and in the crosshairs of a New Lightning War--all the States.

All the States should prepare themselves for all hazards in this age of the Electronic Blitzkrieg.

Sabotage--Kinetic Attacks

Kinetic attacks are a serious threat to the electric grid and are clearly part of the game plan for terrorists and rogue states. Sabotage of the electric grid is perhaps the easiest operation for a terrorist group to execute and would be perhaps the most cost-effective means, requiring only high-powered rifles, for a very small number of bad actors to wage asymmetric warfare--perhaps against all 310 million Americans.

Terrorists have figured out that the electric grid is a major societal vulnerability.

Terror Blackout in Mexico
On the morning of October 27, 2013, the Knights Templars, a terrorist drug cartel in Mexico, attacked a big part of the Mexican grid, using small arms and bombs to blast electric substations. They blacked-out the entire Mexican state of Mihoacan, plunging 420,000 people into the dark, isolating them from help from the Federales. The Knights went into towns and villages and publicly executed local leaders opposed to the drug trade.

Ironically, that evening in the United States, the National Geographic aired a television docudrama "American Blackout" that accurately portrayed the catastrophic consequences of a cyber attack that blacks-out the U.S. grid for ten days. The North American Electric Reliability Corporation and some utilities criticized "American Blackout" for being alarmist and unrealistic, apparently unaware that life had already anticipated art just across the porous border in Mexico.

Life had already anticipated art months earlier than "American Blackout", and not in Mexico, but in the United States.

The Metcalf Attack
On April 16, 2013, apparently terrorists or professional saboteurs practiced making an attack on the Metcalf transformer substation outside San Jose, California, that services a 450 megawatt power plant providing electricity to the Silicon Valley and the San Francisco area. NERC and the utility Pacific Gas and Electric (PG&E), that owns Metcalf, claimed that the incident was merely an act of vandalism, and discouraged press interest.

Consequently, the national press paid nearly no attention to the Metcalf affair for nine months.

Jon Wellinghoff, Chairman of the U.S. Federal Energy Regulatory Commission, conducted an independent investigation of Metcalf. He brought in the best of the best of U.S. special forces--the instructors who train the U.S. Navy SEALS. They concluded that the attack on Metcalf was a highly professional military operation, comparable to what the SEALS themselves would do when attacking a power grid.

Footprints suggested that a team of perhaps as many as six men executed the Metcalf operation. They knew about an underground communications tunnel at Metcalf and knew how to access it by removing a manhole cover (which required at least two men). They cut communications cables and the 911 cable to isolate the site. They had pre-surveyed firing positions. They used AK-47s, the favorite assault rifle of terrorists and rogue states. They knew precisely where to shoot to maximize damage to the 17 transformers at Metcalf. They escaped into the night just as the police arrived and have not been apprehended or even identified. They left no fingerprints anywhere, not even on the expended shell casings.

The Metcalf assailants only damaged but did not destroy the transformers--apparently deliberately. The Navy SEALS and U.S. FERC Chairman Wellinghoff concluded that the Metcalf operation was a "dry run", like a military exercise, practice for a larger and more ambitious attack on the grid to be executed in the future.

Military exercises never try to destroy the enemy, and try to keep a low profile so that the potential victim is not moved to reinforce his defenses. For example, Russian strategic bomber exercises only send a few aircraft to probe U.S. air defenses in Alaska, and never actually launch nuclear-armed cruise missiles. They want to probe and test our air defenses--not scare us into strengthening those defenses.

Chairman Wellinghoff was aware of an internal study by U.S. FERC that concluded saboteurs could blackout the national electric grid for weeks or months by destroying just nine crucial transformer substations.

Much to his credit, Jon Wellinghoff became so alarmed by his knowledge of U.S. grid vulnerability, and the apparent NERC cover-up of the Metcalf affair, that he resigned his chairmanship to warn the American people in a story published by the Wall Street Journal in February 2014. The Metcalf story sparked a firestorm of interest in the press and investigations by Congress.

Consequently, NERC passed, on an emergency basis, a new standard for immediately upgrading physical security for the national electric grid. PG&E promised to spend over $100 million over the next three years to upgrade physical security.

Terror Blackout of Yemen

On June 9, 2014, while world media attention was focused on the terror group Islamic State in Iraq and Syria (ISIS) overrunning northern Iraq, Al Qaeda in the Arabian Peninsula (AQAP) used mortars and rockets to destroy electric transmission towers to blackout all of Yemen, a nation of 16 cities and 24 million people.

AQAP's operation against the Yemen electric grid is the first time in history that terrorists have sunk an entire nation into blackout. The blackout went virtually unreported by the world press.

Metcalf Again--NERC and Utilities Negligent

Two months later, amid growing fears that ISIS may somehow act on its threats to attack America, on August 27, 2014, parties unknown again broke into the Metcalf transformer substation and escaped PG&E security guards and the police. PG&E claims that the second Metcalf affair is, again, merely vandalism.

Yet after NERC's emergency new physical security standards and PG&E's alleged massive investment in improved security--Metcalf should have been the Rock of Gibraltar of the North American electric grid. If terrorists or someone is planning an attack on the U.S. electric grid, Metcalf would be the perfect place to test the supposedly strengthened security of the national grid.

Does stolen equipment prove that Metcalf-2 was a burglary? In the world of spies and saboteurs, mock burglary is a commonplace device for covering-up an intelligence operation, and hopefully quelling fears and keeping the victim unprepared.

If PG&E is telling the truth, and the second successful operation against Metcalf is merely by vandals--this is an engraved invitation by ISIS or Al Qaeda or rogue states to attack the U.S. electric grid. It means that all of PG&E and NERC's vaunted security improvements cannot protect Metcalf from the stupidest of criminals, let alone from terrorists.

About one month later, on September 23, 2014, another investigation of PG&E security at transformer substations, including Metcalf, reported that the transformer substations are still not secure. Indeed, at one site a gate was left wide open. Former CIA Director R. James Woolsey, after reviewing the investigation results, concluded, "Overall, it looks like there is essentially no security."

States Should EMP Harden Their Grids

State governments and their Public Utility Commissions should exercise aggressive oversight to ensure that the transformer substations and electric grids in their States are safe and secure. The record of NERC and the electric utilities indicates they cannot be trusted to provide for the security of the grid.

State governments can protect their grid from sabotage by the "all hazards" strategy that protects against the worst threat--nuclear EMP attack.

For example, faraday cages to protect EHV transformers and SCADAS colonies from EMP would also screen from view these vital assets so they could not be accurately targeted by high-powered rifles, as is necessary in order to destroy them by small arms fire. The faraday cages could be made of heavy metal or otherwise fortified for more robust protection against more powerful weapons, like rocket propelled grenades.

Surge arrestors to protect EHV transformers and SCADAS from nuclear EMP would also protect the national grid from collapse due to sabotage. The U.S. FERC scenario where terrorists succeed in collapsing the whole national grid by destroying merely nine transformer substations works only because of cascading overvoltage. When the nine key substations are destroyed, megawatts of electric power gets suddenly dumped onto other transformers, which in their turn get overloaded and fail, dumping yet more megawatts onto the grid. Cascading failures of more and more transformers ultimately causes a protracted national blackout.

This worst case scenario for sabotage could not happen if the transformers and SCADAS are protected against nuclear EMP--which is a more severe threat than any possible system-generated overvoltage.

Cyber Attack

Cyber attacks, the use of computer viruses and hacking to invade and manipulate information systems and SCADAS, is almost universally described by U.S. political and military leaders as the greatest threat facing the United States. Every day, literally thousands of cyber attacks are made on U.S. civilian and military systems, most of them designed to steal information.

Joint Chiefs Chairman, General Martin Dempsey, warned on June 27, 2013, that the United States must be prepared for the revolutionary threat represented by cyber warfare (Claudette

Roulo, *DoD News*, Armed Force Press Service): "One thing is clear. Cyber has escalated from an issue of moderate concern to one of the most serious threats to our national security," cautioned Chairman Dempsey, "We now live in a world of weaponized bits and bytes, where an entire country can be disrupted by the click of a mouse."

Cyber Hype?

Skeptics claim that the catastrophic scenarios envisioned for cyber warfare are grossly exaggerated, in part to justify costly cyber programs wanted by both the Pentagon and industry at a time of scarce defense dollars. Many of the skeptical arguments about the limitations of hacking and computer viruses are technically correct.

However, it is not widely understood that foreign military doctrines define "information warfare" and "cyber warfare" as encompassing kinetic attacks and EMP attack--which is an existential threat to the United States.

Thomas Rid's book *Cyber War Will Not Take Place* (Oxford University Press, 2013) exemplifies the viewpoint of a growing minority of highly talented cyber security experts and scholars who think there is a conspiracy of governments and industry to hype the cyber threat. Rid's bottom line is that hackers and computer bugs are capable of causing inconvenience--not apocalypse. Cyber attacks can deny services, damage computers selectively but probably not wholesale, and steal information, according to Rid. He does not rule out that future hackers and viruses could collapse the electric grid, concluding such a feat would be, not impossible, but nearly so.

In a 2012 BBC interview, Rid chastised then Secretary of Defense Leon Panetta for claiming that Iran's Shamoon Virus, used against the U.S. banking system and Saudi Arabia's ARAMCO, could foreshadow a "Cyber Pearl Harbor" and for threatening military retaliation against Iran. Rid told the BBC that the world has, "Never seen a cyber attack kill a single human being or destroy a building."

Cyber security expert Bruce Schneier claims, "The threat of cyberwar has been hugely hyped" to keep growing cyber security programs at the Pentagon's Cyber Command, the Department of Homeland Security, and new funding streams to Lockheed Martin, Raytheon, Century Link, and AT&T, who are all part of the new cyber defense industry. The Brookings Institute's Peter Singer wrote in November 2012, "Zero. That is the number of people who have been hurt or killed by cyber terrorism." Ronald J. Delbert, author of *Black Code: Inside the Battle for Cyberspace*, a lab director and professor at the University of Toronto, accuses RAND and the U.S. Air Force of exaggerating the threat from cyber warfare.

Peter Sommer of the London School of Economics and Ian Brown of Oxford University, in *Reducing Systemic Cybersecurity Risk*, a study for Europe's Organization for Economic Cooperation and Development, are far more worried about natural EMP from the Sun than computer viruses: "a catastrophic cyber incident, such as a solar flare that could knock out satellites, base stations and net hardware" makes computer viruses and hacking "trivial in comparison."

Aurora Experiment
The now declassified Aurora experiment is the empirical basis for the claim that a computer virus might be able to collapse the national electric grid. In Aurora, a virus was inserted into the SCADAS running a generator, causing the generator to malfunction and eventually destroy itself.

However, using a computer virus to destroy a single generator does not prove it is possible or likely that an adversary could destroy all or most of the generators in the United States. Aurora took a protracted time to burn out a generator--and no intervention by technicians attempting to save the generator was allowed, as would happen in a nationwide attack, if one could be engineered.

Nor is there a single documented case of a even a local blackout being caused in the United States by a computer virus or hacking--which surely would have happened by now, if vandals, terrorists, or rogue states could attack U.S. critical infrastructures easily by hacking.

Stuxnet Worm and Gaza Cyber War
Even the Stuxnet Worm, the most successful computer virus so far, reportedly according to White House sources jointly engineered by the U.S. and Israel to attack Iran's nuclear weapons program, proved a disappointment. Stuxnet succeeded in damaging only 10 percent of Iran's centrifuges for enriching uranium, and did not stop or even significantly delay Tehran's march towards the bomb.

During the recently concluded Gaza War between Israel and Hamas, a major cyber campaign using computer bugs and hacking was launched against Israel by Hamas, the Syrian Electronic Army, Iran, and by sympathetic hackers worldwide. The Gaza War was a Cyber World War against Israel.

The Institute for National Security Studies, at Tel Aviv University, in "The Iranian Cyber Offensive during Operation Protective Edge" (August 26, 2014) reports that the cyber attacks caused inconvenience and in the worst case some alarm, over a false report that the Dimona nuclear reactor was leaking radiation: "...the focus of the cyber offensive...was the civilian internet. Iranian elements participated in what the C4I officer described as an attack unprecedented in its proportions and the quality of its targets....The attackers had some success when they managed to spread a false message via the IDF's official Twitter account saying that the Dimona reactor had been hit by rocket fire and that there was a risk of a radioactive leak."

However, the combined hacking efforts of Hamas, SEA, Iran and hackers worldwide did not blackout Israel or significantly impede Israel's war effort.

Dragonfly
But tomorrow is always another day. Cyber warriors are right to worry that perhaps someday someone will develop the cyber bug version of an atomic bomb. Perhaps such a computer virus already exists in a foreign laboratory, awaiting use in a future surprise attack.

On July 6, 2014, reports surfaced that Russian intelligence services allegedly infected 1,000 power plants in Western Europe and the United States with a new computer virus called

Dragonfly. No one knows what Dragonfly is supposed to do. Some analysts think it was just probing the defenses of western electric grids. Others think Dragonfly may have inserted logic bombs into SCADAS that can disrupt the operation of electric power plants in a future crisis.

States Should EMP Harden Their Grids

Cyber warfare is an existential threat to the United States, not because of computer viruses and hacking alone, but as envisioned in the military doctrines of potential adversaries whose plans for an all-out Cyber Warfare Operation include the full spectrum of military capabilities--including EMP attack. In 2011, a U.S. Army War College study *In The Dark: Planning for a Catastrophic Critical Infrastructure Event* warned U.S. Cyber Command that U.S. doctrine should not overly focus on computer viruses to the exclusion of EMP attack and the full spectrum of other threats, as planned by potential adversaries.

Reinforcing the above, a Russian technical article on cyber warfare by Maxim Shepovalenko (*Military-Industrial Courier* July 3, 2013), notes that a cyber attack can collapse "the system of state and military control...its military and economic infrastructure" because of "electromagnetic weapons...an electromagnetic pulse acts on an object through wire leads on infrastructure, including telephone lines, cables, external power supply and output of information."

Cyber warriors who think narrowly in terms of computer hacking and viruses invariably propose anti-hacking and anti-viruses as solutions. Such a solution will result in an endless virus versus anti-virus software arms race that may ultimately prove unaffordable and futile.

States can protect themselves from the worst case cyber scenario by following the "all hazards" strategy recommended by the Congressional EMP Commission. The worst case scenario envisions a computer virus infecting the SCADAS that regulate the flow of electricity into EHV transformers, damaging the transformers with overvoltage, and causing a protracted national blackout.

But if the transformers are protected with surge arrestors against the worst threat--nuclear EMP attack--they would be unharmed by the worst possible overvoltage that might be system generated by any computer virus. This EMP hardware solution would provide a permanent and relatively inexpensive fix to what is the extremely expensive and apparently endless virus versus anti-virus software arms race that is ongoing in the new cyber defense industry.

EMP Attack

High-altitude nuclear electromagnetic pulse attack is the most severe threat to the electric grid and other critical infrastructures. A nuclear EMP attack would likely be more damaging than a geomagnetic super-storm, the worst case of severe weather, sabotage by kinetic attacks, or cyber attack.

Contrary to non-experts sometimes cited in the press, there is more empirical data on nuclear EMP and more analysis and a better understanding of EMP effects on electronic systems and infrastructures than almost any other threat, except severe weather. In addition to the 1962 STARFISH PRIME high-altitude nuclear test that generated EMP that damaged electronic systems in Hawaii and elsewhere, the Department of Defense has decades of atmospheric and

underground nuclear test data relevant to EMP. And defense scientists have for over 50 years studied EMP effects on electronics in simulators. Most recently, the Congressional EMP Commission made its threat assessment by testing a wide range of modern electronics crucial to critical infrastructures in EMP simulators.

There is a scientific and strategic consensus behind the Congressional EMP Commission's assessment that a nuclear EMP attack would have catastrophic consequences for the United States, but that "correction is feasible and well within the Nation's means and resources to accomplish." Every major U.S. Government study to examine the EMP threat and solutions concurs with the EMP Commission, including the Congressional Strategic Posture Commission (2009), the U.S. Department of Energy and North American Electric Reliability Corporation (2010), and the U.S. Federal Energy Regulatory Commission interagency report, coordinated with the White House, Department of Defense, and Oak Ridge National Laboratory (2010).

Not one major U.S. Government study dissents from the consensus that nuclear EMP attack would be catastrophic, and that protection is achievable and necessary.

Russian Nuclear EMP Tests
STARFISH PRIME is not the only high-altitude nuclear EMP test.

The Soviet Union (1961-1962) conducted a series of high-altitude nuclear EMP tests over what was then its own territory--not once but seven times--using a variety of warheads of different designs. The EMP fields from six tests covered Kazakhstan, an industrialized area larger than Western Europe. In 1994, during a thaw in the Cold War, Russia shared the results from one of its nuclear EMP tests, that used their least efficient warhead design for EMP--it collapsed the Kazakhstan electric grid, damaging transformers, generators and all other critical components.

The USSR during the Kazakhstan high-altitude EMP experiments tested some low-yield warheads, at least one probably an Enhanced Radiation Warhead that emitted large quantities of gamma rays, that generate the E1 EMP electromagnetic shockwave. It is possible that the USSR developed their Super-EMP Warhead early in the Cold War as a secret super-weapon.

Perhaps the most important lesson to be learned from the USSR's unconscionable and evil nuclear EMP tests against their own people is that there is no excuse to be vulnerable to EMP. The Soviets apparently quickly repaired the damage to Kazakhstan's electric grid and other critical infrastructures, thereby proving definitively that with smart planning and good preparedness it is possible to survive and recover from an EMP catastrophe.

Nuclear EMP Attacks by Missile, Aircraft and Balloon
A nuclear weapon detonated at an altitude of 200 kilometers over the geographic center of the United States would create an EMP field potentially damaging to electronics over all the 48 contiguous States. The Congressional EMP Commission concluded that virtually any nuclear weapon, even a crude first generation atomic bomb having a low yield, could potentially inflict an EMP catastrophe.

However, the EMP Commission also found that Russia, China, and probably North Korea have nuclear weapons specially designed to generate extraordinarily powerful EMP fields-- called by the Russians Super-EMP weapons--and this design information may be widely proliferated: "Certain types of relatively low-yield nuclear weapons can be employed to generate potentially catastrophic EMP effects over wide geographic areas, and designs for variants of such weapons may have been illicitly trafficked for a quarter-century."

Nor is a sophisticated long-range missile required to make an EMP attack.

Any short-range missile or other delivery vehicle that can deliver a nuclear weapon to an altitude of 30 kilometers or higher can make a potentially catastrophic EMP attack on the United States. Although a nuclear weapon detonated at 30 kilometers altitude could not cover the entire continental U.S. with an EMP field, the field would still cover a very large multi-state region--and be more intense. Lowering the height-of-burst (HOB) for an EMP attack decreases field radius, but increases field strength.

An EMP attack at 30 kilometers HOB anywhere over the eastern half of the U.S. would cause cascading failures far beyond the EMP field and collapse the Eastern Grid, that generates 75 percent of U.S. electricity. The nation could not survive without the Eastern Grid.

A Scud missile launched from a freighter could perform such an EMP attack. Over 30 nations have Scuds, as do some terrorist groups and private collectors. Scuds are available for sale on the world and black markets.

Any aircraft capable of flying Mach 1 could probably do a zoom climb to 30 kilometers altitude to make an EMP attack, if the pilot is willing to commit suicide.

Even a meteorological balloon could be used to loft a nuclear weapon 30 kilometers high to make an EMP attack. During the period of atmospheric nuclear testing in the 1950s and early 1960s, more nuclear weapons were tested at altitude by balloon than by bombers or missiles.

Nuclear EMP Effects on Critical Infrastructures

Nuclear EMP is like super-lightning. The electromagnetic shockwave unique to nuclear weapons, called E1 EMP, travels at the speed of light, potentially injecting into electrical systems thousands of volts in a nanosecond--literally a million times faster than lightning, and much more powerful. Russian open source military writings describe their Super-EMP Warhead as generating 200,000 volts/meter, which means that the target receives 200,000 volts for every meter of its length. So, for example, if the cord on a PC is two meters long, it receives 400,000 volts. An automobile 4 meters long could receive 800,000 volts, unless it is parked underground or protected in some other way.

No other threat can cause such broad and deep damage to all the critical infrastructures as a nuclear EMP attack. A nuclear EMP attack would collapse the electric grid, blackout and directly damage transportation systems, industry and manufacturing, telecommunications and computers, banking and finance, and the infrastructures for food and water.

Jetliners carry about 500,000 passengers on over 1,000 aircraft in the skies over the U.S. at any given moment. Many, most or virtually all of these would crash, depending upon the strength of the EMP field. Satellite navigation and communication systems would be knocked out, as would ground and air traffic control systems, necessitating that any surviving aircraft land "blind."

Cars, trucks, trains and traffic control systems would be damaged. In the best case, even if only a few percent of ground transportation vehicles are rendered inoperable, massive traffic jams would result. In the worst case, virtually all vehicles of all kinds would be rendered inoperable. In any case, all vehicles would stop operating when they run out of gasoline. The blackout would render gas stations inoperable and paralyze the infrastructure for synthesizing and delivering petroleum products and fuels of all kinds.

Industry and manufacturing would be paralyzed by collapse of the electric grid. Damage to SCADAS and safety control systems would likely result in widespread industrial accidents, including gas line explosions, chemical spills, fires at refineries and chemical plants producing toxic clouds.

Seven days after the commencement of blackout, emergency generators at nuclear reactors would run out of fuel. The reactors and nuclear fuel rods in cooling ponds would meltdown and catch fire, as happened in the nuclear disaster at Fukushima, Japan. The 104 U.S. nuclear reactors, located mostly among the populous eastern half of the United States, could cover vast swaths of the nation with dangerous plumes of radioactivity.

Cell phones, personal computers, the internet, and the modern electronic economy that supports personal and big business cash, credit, debit, stock market and other transactions and record keeping would cease operations. The Congressional EMP Commission warns that society could revert to a barter economy.

Worst of all, about 72 hours after the commencement of blackout, when emergency generators at the big regional food warehouses cease to operate, the nation's food supply will begin to spoil. Supermarkets are resupplied by these large regional food warehouses that are, in effect, the national larder, collectively having enough food to sustain the lives of 310 million Americans for about one month, at normal rates of consumption. The Congressional EMP Commission warns that as a consequence of the collapse of the electric grid and other critical infrastructures, "It is possible for the functional outages to become mutually reinforcing until at some point the degradation of infrastructure could have irreversible effects on the country's ability to support its population."

The EMP Commission estimates that a nationwide blackout lasting one year could kill up to 9 of 10 Americans through starvation, disease, and societal collapse.

Nuclear EMP Threat Is Real

The nuclear EMP threat is not merely theoretical, but real.

"China and Russia have considered limited nuclear attack options that, unlike their Cold War plans, employ EMP as the primary or sole means of attack," according to the Congressional EMP

Commission, "Indeed, as recently as May 1999, during the NATO bombing of the former Yugoslavia, high-ranking members of the Russian Duma, meeting with a U.S. congressional delegation to discuss the Balkans conflict, raised the specter of a Russian EMP attack that would paralyze the United States."

Russia has made many nuclear threats against the U.S. since 1999, which are reported in the western press only rarely. On December 15, 2011, Pravda, the official mouthpiece of the Kremlin, gave this advice to the United States in "A Nightmare Scenario For America":

> *No missile defense could prevent...EMP...No one seriously believes that U.S. troops overseas are defending "freedom" or defending their country.... Perhaps they ought to close the bases, dismantle NATO and bring the troops home where they belong before they have nothing to come home to and no way to get there.*

On June 1, 2014, Russia Today, a Russian television news show, also broadcast to the West in English, predicted that the United States and Russia would be in a nuclear war by 2016.

Iran, the world's leading sponsor of international terrorism, openly writes about making a nuclear EMP attack to eliminate the United States. Iran has practiced missile launches that appear to be training and testing warhead fusing for a high-altitude EMP attack--including missile launching for an EMP attack from a freighter. An EMP attack launched from a freighter could be performed anonymously, leaving no fingerprints, to foil deterrence and escape retaliation.

"What is different now is that some potential sources of EMP threats are difficult to deter--they can be terrorist groups that have no state identity, have only one or a few weapons, and are motivated to attack the U.S. without regard for their own safety," cautions the EMP Commission in its 2004 report, "Rogue states, such as North Korea and Iran, may also be developing the capability to pose an EMP threat to the United States, and may also be unpredictable and difficult to deter."

On April 16, 2013, North Korea apparently simulated a nuclear EMP attack against the United States, orbiting its KSM-3 satellite over the U.S. at the optimum trajectory and altitude to place a peak EMP field over Washington and New York and blackout the Eastern Grid, that generates 75 percent of U.S. electricity. On the very same day, as described earlier, parties unknown executed a highly professional commando-style sniper attack on the Metcalf transformer substation that is a key component of the Western Grid.

A few months later, in July 2013, North Korean freighter *Chon Chong Gang* transited the Gulf of Mexico carrying nuclear-capable SA-2 missiles in its hold on their launchers. The missiles had no warheads, but the event demonstrated North Korea's capability to execute a ship-launched nuclear EMP attack from U.S. coastal waters anonymously, to escape U.S. retaliation. The missiles were only discovered, hidden under bags of sugar, because the freighter tried returning to North Korea through the Panama Canal and past inspectors.

What does all this signify?

Connect these dots: North Korea's apparent practice EMP attack with its KSM-3 satellite; the simultaneous "dry run" sabotage attack at Metcalf; North Korea's possible practice for a ship-launched EMP attack a few months later; and cyber attacks from various sources were happening all the time, and are happening every day. These suggest the possibility that in 2013 at least North Korea may have exercised against the United States an all-out combined arms operation aimed at targeting U.S. critical infrastructures--the New Lightning War.

Or are these coincidences merely accidental?

Is it also mere happenstance that Metcalf services the Silicon Valley, that reportedly developed the Stuxnet Worm that attacked Iran's nuclear program, for which transgression the Iranian Revolutionary Guard swore revenge? Iran and North Korea are by treaty strategic partners and closely cooperate in their scientific and military programs. With North Korean help, Iran too has orbited satellites on trajectories consistent with practicing a surprise nuclear EMP attack on the United States.

Non-Nuclear EMP Weapons

Radio-Frequency Weapons (RFWs) are non-nuclear weapons that use a variety of means, including explosively driven generators, to emit an electromagnetic pulse similar to the E1 EMP from a nuclear weapon, except less energetic and of much shorter radius. The range of RF Weapons is rarely more than one kilometer.

RF Weapons can be built relatively inexpensively using commercially available parts and design information available on the internet. In 2000 the Terrorism Panel of the House Armed Services Committee conducted an experiment, hiring an electrical engineer and some students to try building an RFW on a modest budget, using design information available on the internet, made from parts purchased at Radio Shack.

They built two RF Weapons in one year, both successfully tested at the U.S. Army proving grounds at Aberdeen. One was built into a Volkswagen bus, designed to be driven down Wall Street to disrupt stock market computers and information systems and bring on a financial crisis. The other was designed to fit in the crate for a Xerox machine so it could be shipped to the Pentagon, sit in the mailroom, and burn-out Defense Department computers.

EMP simulators that can be carried and operated by one man, and used as an RF Weapon, are available commercially. For example, one U.S. company advertises for sale an "EMP Suitcase" that looks exactly like a metal suitcase, can be carried and operated by one man, and generates 100,000 volts/meter over a short distance. The EMP Suitcase is not intended to be used as a weapon, but as an aid for designing factories that use heavy duty electronic equipment that emit electromagnetic transients, so the factory does not self-destruct.

But a terrorist, criminal, or madman, armed with the EMP Suitcase, could potentially destroy electric grid SCADAS or an EHV transformer and blackout a city. Thanks to RF Weapons, we have arrived at a place where the technological pillars of civilization for a major metropolitan area could be toppled by a single individual.

The EMP Suitcase can be purchased without a license by anyone.

Terrorists armed with RF Weapons might use unclassified computer models to duplicate the U.S. FERC study and figure out which nine crucial transformer substations need to be attacked in order to blackout the entire national grid for weeks or months. RFWs would offer significant operational advantages over assault rifles and bombs. Something like the EMP Suitcase could be put in the trunk of a car, parked and left outside the fence of an EHV transformer or SCADA colony, or hidden in nearby brush or a garbage can, while the bad guys make a leisurely getaway. If the EMP fields are strong enough, it would be just as effective as, and far less conspicuous than, dropping a big bomb to destroy the whole transformer substation. Maximum effect could be achieved by penetrating the security fence and hiding the RF Weapon somewhere even closer to the target.

Some documented examples of successful attacks using Radio Frequency Weapons, and accidents involving electromagnetic transients, are described in the Department of Defense *Pocket Guide for Security Procedures and Protocols for Mitigating Radio Frequency Threats* (Technical Support Working Group, Directed Energy Technical Office, Dahlgren Naval Surface Warfare Center):

--"In the Netherlands, an individual disrupted a local bank's computer network because he was turned down for a loan. He constructed a Radio Frequency Weapon the size of a briefcase, which he learned how to build from the Internet. Bank officials did not even realize that they had been attacked or what had happened until long after the event."
--"In St. Petersburg, Russia, a criminal robbed a jewelry store by defeating the alarm system with a repetitive RF generator. Its manufacture was no more complicated than assembling a home microwave oven."
--"In Kzlyar, Dagestan, Russia, Chechen rebel commander Salman Raduyev disabled police radio communications using RF transmitters during a raid."
--"In Russia, Chechen rebels used a Radio Frequency Weapon to defeat a Russian security system and gain access to a controlled area."
-- "Radio Frequency Weapons were used in separate incidents against the U.S. Embassy in Moscow to falsely set off alarms and to induce a fire in a sensitive area."
--"March 21-26, 2001, there was a mass failure of keyless remote entry devices on thousands of vehicles in the Bremerton, Washington, area...The failures ended abruptly as federal investigators had nearly isolated the source. The Federal Communications Commission (FCC) concluded that a U.S. Navy presence in the area probably caused the incident, although the Navy disagreed."
--"In 1999, a Robinson R-44 news helicopter nearly crashed when it flew by a high frequency broadcast antenna."
--"In the late 1980s, a large explosion occurred at a 36-inch diameter natural gas pipeline in the Netherlands. A SCADA system, located about one mile from the naval port of Den Helder, was affected by a naval radar. The RF energy from the radar caused the SCADA system to open and close a large gas flow-control valve at the radar scan frequency, resulting in pressure waves that traveled down the pipe and eventually caused the pipeline to explode."

--"In June 1999 in Bellingham, Washington, RF energy from a radar induced a SCADA malfunction that caused a gas pipeline to rupture and explode."
--"In 1967, the *USS Forrestal* was located at Yankee Station off Vietnam. An A4 Skyhawk launched a Zuni rocket across the deck. The subsequent fire took 13 hours to extinguish. 134 people died in the worst U.S. Navy accident since World War II. EMI [Electro-Magnetic Interference, Pry] was identified as the probable cause of the Zuni launch."
--North Korea used an Radio Frequency Weapon, purchased from Russia, to attack airliners and impose an "electromagnetic blockade" on air traffic to Seoul, South Korea's capitol. The repeated attacks by RFW also disrupted communications and the operation of automobiles in several South Korean cities in December 2010; March 9, 2011; and April-May 2012 as reported in "Massive GPS Jamming Attack By North Korea" (*GPSWORLD.COM*, May 8, 2012).

Protecting the electric grid and other critical infrastructures from nuclear EMP attack will also protect them from the lesser threat posed by Radio Frequency Weapons.

States Should EMP Harden Their Grids
States should harden their electric grids against nuclear EMP attack because there is a clear and present danger, because protecting against nuclear EMP will mitigate all lesser threats, and because both the federal government in Washington and the electric power industry have failed to protect the people from the existential peril that is an EMP catastrophe.

In the U.S. Congress, bipartisan bills with strong support, such as the GRID Act and the SHIELD Act, that would protect the electric grid from nuclear and natural EMP, have been stalled for a half-decade, blocked by corruption and lobbying by powerful utilities.

The U.S. Federal Energy Regulatory Commission has published interagency reports acknowledging that nuclear EMP attack is an existential threat against which the electric grid must be protected. But U.S. FERC claims to lack legal authority to require the North American Electric Reliability Corporation and the electric utilities to protect the grid.

"Given the national security dimensions to this threat, there may be a need to act quickly to act in a manner where action is mandatory rather than voluntary and to protect certain information from public disclosure," said Joseph McClelland, Director of FERC's Office of Energy Projects, testifying in May 2011 before the Senate Energy and Natural Resources Committee. "The commission's legal authority is inadequate for such action."

Others think U.S. FERC has sufficient legal authority to protect the grid, but lacks the will to do so because of an incestuous relationship with the NERC.

NERC and the electric power industry deny that it is their responsibility to protect the grid from nuclear EMP attack. NERC thinks it is not their job, but the job of the Department of Defense, to protect the United States from nuclear EMP attack, so argued NERC President and CEO, Gerry Cauley, in his May 2011 testimony before the Senate Energy and Natural Resources Committee. Mark Lauby, NERC's reliability manager, is quoted by Peter Behr in his *EENEWS* article (August 26, 2011) that "...the terrorist scenario--foreseen as the launch of a crude nuclear

weapon on a version of a SCUD missile from a ship off the U.S. coast--is the government's responsibility, not industry's."

But DOD can protect the grid only by waging preventive wars against countries like Iran, North Korea, China and Russia, or by vast expansion and improvement of missile defenses costing tens of billions of dollars--none of which may stop the EMP threat.

Preventive wars would make an EMP attack more likely, perhaps inevitable. It is not worth spending thousands of lives and trillions of dollars on wars, just so NERC and the utilities can avoid a small increase in electric bills for EMP hardening the grid. U.S. FERC estimates EMP hardening would cost the average ratepayer an increase in their electric bill of 20 cents annually.

The Department of Defense has no legal authority to EMP harden the privately owned electric grid. Such protection is supposed to be the job of NERC and the utilities.

Most alarming, NERC and the utilities do not appear to know their jobs, and are already in panic and despair over the challenges posed by severe weather, cyber threats, and geomagnetic storms. Peter Behr in an article published in *Energy Wire* (September 12, 2014) reports that at an electric grid security summit, Gary Leidich, Board Chairman of the Western Electricity Coordinating Council--which oversees reliability and security for the Western Grid--appears overwhelmed, as if he wants to escape his job, crying: "Who is really responsible for reliability? And who has the authority to do something about it?"

"The biggest cyber threat is from an electromagnetic pulse, which in the military doctrines of our potential adversaries would be part of an all-out cyber war.", writes former Speaker of the House, Newt Gingrich, in his article "The Gathering Cyber Storm" (*CNN*, August 12, 2013). Gingrich warns that NERC "should lead, follow or get out of the way of those who are trying to protect our nation from a cyber catastrophe. Otherwise, the Congress that certified it as the electric reliability organization can also decertify it."

Much to their credit, a few in the electric power industry understand the necessity of protecting the grid from nuclear EMP attack, have broken ranks with NERC, and are trying to meet the crisis. John Houston of Centerpoint Energy in Texas; Terry Boston of PJM, the largest grid in North America (located in the midwest); and Con Ed in New York--all are trying to protect their grids from nuclear EMP.

State Governors and State Legislatures need to come to the rescue. States have a duty to their citizens to fill the gap in homeland security and public safety when the federal government, and the utilities, fail.

State governments and their Public Utility Commissions have the legal authority and the moral obligation to, where necessary, compel the utilities to secure the grid against all hazards. State governments have an obligation to help and oversee and ensure that grid security is being done right by those utilities that act voluntarily.

Failing to protect the grid from nuclear EMP attack is failing to protect the nation from all hazards.

Regulatory Malfeasance

As noted repeatedly elsewhere, Washington's process for regulating the electric power industry has never worked well, in fact has always been broken. The electric power industry is the only civilian critical infrastructure that is allowed to regulate itself.

The North American Electric Reliability Corporation is the industry's former trade association, which continues to act as an industry lobby. NERC is not a U.S. government agency. It does not represent the interests of the people. NERC in its charter answers to its "stakeholders"--the electric utilities that pay for NERC, including NERC's highly salaried executives and staff.

The U.S. Federal Energy Regulatory Commission, the U.S. government agency that is supposed to partner with NERC in protecting the national electric grid, has publicly testified before Congress that U.S. FERC lacks regulatory power to compel NERC and the electric power industry to protect the grid from natural and nuclear EMP and other threats.

Consider the contrast in regulatory authority between the U.S. FERC and, as examples, the U.S. Federal Aviation Administration (FAA), the U.S. Department of Transportation (DOT), or the U.S. Food and Drug Administration (FDA):

--FAA has regulatory power to compel the airlines industry to ground aircraft considered unsafe, to change aircraft operating procedures considered unsafe, and to make repairs or improvements to aircraft in order to protect the lives of airline passengers.
--DOT has regulatory power to compel the automobile industry to install on cars safety glass, seatbelts, and airbags in order to protect the lives of the driving public.
--FDA has power to regulate the quality of food and drugs, and can ban under criminal penalty the sale of products deemed by the FDA to be unsafe to the public.

Unlike the FAA, DOT, FDA or any other U.S. government regulatory agency, the Federal Energy Regulatory Commission does not have legal authority to compel the industry it is supposed to regulate to act in the public interest. For example, U.S. FERC lacks legal power to direct NERC and the electric utilities to install blocking devices, surge arrestors, faraday cages or other protective devices to save the grid, and the lives of millions of Americans, from a natural or nuclear EMP catastrophe. Or so the FERC has testified to the Congress.

Congress has responded to this dilemma by introducing bipartisan bills, the SHIELD Act and the GRID Act, to empower U.S. FERC to protect the grid from an EMP catastrophe. Lobbying by NERC has stalled both bills for years.

Currently, U.S. FERC only has the power to ask NERC to propose a standard to protect the grid. NERC standards are approved, or rejected, by the electric power industry.

Historically, NERC typically takes years to develop standards to protect the grid that will pass industry approval. For example, NERC took a decade to propose a "vegetation management"

standard to protect the grid from tree branches in 2012. This after ruminating for ten years over the tree branch induced Great Northeast Blackout of 2003, that plunged 50 million Americans into the dark.

Once NERC proposes a standard to U.S. FERC, FERC cannot modify the standard, but must accept or reject the proposed standard. If U.S. FERC rejects the proposed standard, NERC gets to go back to the drawing board, and the process starts all over again.

The NERC-FERC arrangement is a formula for thwarting effective U..S. government regulation of the electric power industry. Fortunately, Governors, State Legislatures and their Public Utility Commissions have legal power to compel utilities to protect the grid from natural and nuclear EMP and other threats.

Critics argue that the U.S. Federal Energy Regulatory Commission is corrupt--because of a too cozy relationship with NERC and a rotating door between FERC and the electric power industry--and cannot be trusted to secure the grid, even if given legal powers to do so. U.S. FERC's approval of NERC's hollow standard for geomagnetic storms appears proof positive that Washington is too corrupt to be trusted.

NERC's Hollow GMD Protection Standard

Observers serving on NERC's Geo-Magnetic Disturbance Task Force, that developed the NERC standard for grid protection against geomagnetic storms, have denounced the NERC GMD Standard and published papers exposing, not merely that the Standard is inadequate, but that it is hollow, a pretended or fake Standard. These experts opposed to the NERC GMD Standard include the foremost authorities on geomagnetic storms and electric grid vulnerability in the Free World. See:

--John G. Kappenman and Dr. William A. Radasky, *Examination of NERC GMD Standards and Validation of Ground Models and Geo-Electric Fields Proposed in this NERC GMD Standard*, Storm Analysis Consultants and Metatech Corporation, July 30, 2014 (Executive Summary appended to this chapter).
--*EIS Council Comments on Benchmark GMD Event for NERC GMD Task Force Consideration*, Electric Infrastructure Security Council, May 21, 2014.
--Thomas Popik and William Harris for The Foundation for Resilient Societies, *Reliability Standard for Geomagnetic Disturbance Operations*, Docket No. RM14-1-000, critiques submitted to U.S. FERC on March 24, July 21, and August 18, 2014.

Kappenman and Radasky, who served on the Congressional EMP Commission and are among the world's foremost scientific and technical experts on geomagnetic storms and grid vulnerability, warn that NERC's GMD Standard consistently underestimates the threat from geo-storms: "When comparing...actual geo-electric fields with NERC model derived geo-electric fields, the comparisons show a systematic under-prediction in all cases of the geo-electric field by the NERC model."

The Foundation for Resilient Societies, that includes on its Board of Advisors a brain trust of world class scientific experts--including Dr. William Graham who served as President Reagan's

Science Advisor, director of NASA, and Chairman of the Congressional EMP Commission--concludes from their participation on the NERC GMD Task Force that NERC "cooked the books" to produce a hollow GMD Standard:

> *The electric utility industry clearly recognized in this instance how to design a so-called "reliability standard" that, though foreseeably ineffective in a severe solar storm, would avert financial liability to the electric utility industry even while civil society and its courts might collapse from longer-term outages. In this instance and others, a key feature of the NERC standard-setting process was to progressively water down requirements until the proposed standard obviously benefitted the ballot participants and therefore could pass. In the process, any remaining public benefit was diluted beyond perceptibility...*

The several Foundation critiques identify numerous profound and obvious holes in what it describes as NERC's "hollow" GMD Standard, and rightly castigates U.S. FERC for approving what is, in reality, a paper mache GMD Standard that would not protect the grid from a geomagnetic super-storm:

--"FERC erred by approving a standard that exempts transmission networks with no transformers with a high side (wye-grounded) voltage at or above 200 kV when actual data and lessons learned from past operating incidents show significant adverse impacts of solar storms on equipment operating below 200 kV."
--"The exclusion of networks operating at 200kV and below is inconsistent with the prior bright-line definition of the Bulk Electric System" as defined by U.S. FERC.
--"FERC erred by approving a standard that does not require instrumentation of electric utility networks during solar storm conditions when installation of GIC [Ground Induced Current--Pry] monitors would be cost-effective and in the public interest."
--"FERC erred by approving a standard that does not require utilities to perform the most rudimentary planning for solar storms, i.e., mathematical comparison of megawatt capacity of assets at risk during solar storms to power reserves."
--"FERC erred by concluding that sixteen Reliability Coordinators could directly communicate with up to 1,500 Transmission and Generator Operators during severe GMD events with a warning time of as little as 15 minutes and that Balancing Authorities and Generator Operators should not take action on their own because of possible lack of GIC data."
--"FERC erred by assuming that there would be reliable and prompt two-way communications between Reliability Coordinators and Generator Operators immediately before and during severe solar storms."

The Foundation is also critical of U.S. FERC for approving a NERC GMD Standard that lacks transparency and accountability. The utilities are allowed to assess their own vulnerability to geomagnetic storms, to devise their own preparations, to invest as much or as little as they like in those preparations, and all without public scrutiny or review of utility plans by independent experts.

Dr. William Radasky, who holds the Lord Kelvin Medal for setting standards for protecting European electronics from natural and nuclear EMP, and John Kappenman, who helped design the ACE satellite upon which industry relies for early warning of geomagnetic storms, conclude that the NERC GMD Standard so badly underestimates the threat that "its resulting directives are not valid and need to be corrected." Kappenman and Radasky:

> *These enormous model errors also call into question many of the foundation findings of the NERC GMD draft standard. The flawed geo-electric field model was used to develop the peak geo-electric field levels of the Benchmark model proposed in the standard. Since this model understates the actual geo-electric field intensity for small storms by a factor of 2 to 5, it would also understate the maximum geo-electric field by similar or perhaps even larger levels. Therefore, the flaw is entirely integrated into the NERC Draft Standard and its resulting directives are not valid and need to be corrected.*

The excellent Kappenman-Radasky critique of the NERC GMD Standard represents the consensus view of all the independent observers who participated in the NERC GMD Task Force, including the author. The Kappenman-Radasky critique warns NERC and U.S. FERC that, "Nature cannot be fooled!"

Perhaps most revelatory of U.S. FERC's untrustworthiness, by approving the NERC GMD Standard that grossly underestimates the threat from geo-storms--U.S. FERC abandoned its own much more realistic estimate of the geo-storm threat. It is incomprehensible why U.S. FERC would ignore the findings of its own excellent interagency study, one of the most in depth and meticulous studies of the EMP threat ever performed, that was coordinated with Oak Ridge National Laboratory, the Department of Defense, and the White House.

U.S. FERC's preference for NERC's "junk science" over U.S. FERC's own excellent scientific assessment of the geo-storm threat can only be explained as incompetence or corruption or both.

The bottom line is that the people and the States cannot trust NERC and U.S. FERC to protect the national electric grid from natural EMP. They probably cannot trust NERC and the U.S. FERC to protect the grid from anything.

States should protect their own electric grids, and their people who depend upon the grid for survival, from the worst threat--nuclear EMP attack--so they will be ready for everything.

Mr. DESANTIS. Thank you. Mr. Caruso, thank you for coming you're recognized for 5 minutes.

STATEMENT OF MICHAEL CARUSO

Mr. CARUSO. Thank you. I'd like to thank Chairman DeSantis, Chairman Lummis, ranking members and committee members for this opportunity to testify. I consider it an honor and a privilege to be here today to share my 32 years of experience in the practical side of protecting against EMP events.

EMP hardening has long been considered very expensive and an illusive art known to few. The current guidance on EMP protection is found in the MIL Standard 188–125 that is not necessarily appropriate for every application when considering the critical infrastructure.

EMP hardening of the critical infrastructure would require a less stringent application of the MIL Standard 188–125. Government, public, and private critical infrastructure facilities and services are becoming increasingly interdependent, as we've seen with many of the companies that I've talked to over the past 3 years.

In addition to the interdependency of those services, we see an increasingly dependence on the very vulnerable electric grid and electric power system. To date, little has been done to harden the electric power system and the 16 segments of critical infrastructure as designated by the Department of Homeland Security.

Currently, 18 States have ongoing initiatives to require the electric utilities to at least address the protection of the electrical grid from the dangers of a EMP or solar storm. Electromagnetic energy from an EMP can disrupt a supervisory and control data acquisition systems, or SCADA systems, which the electric grid heavily relies.

I recently testified in the Texas State House in support of bills introduced for EMP protection of the critical infrastructure. Texas is one of the States aggressively pursuing passage of EMP legislation, including an appropriation to get critical infrastructure segments started in the overall evaluation of their vulnerability.

In 2014, ETS–Lindgren, the company for which I work, was part of a multidisciplinary team that successfully completed construction of the very first large private sector SCADA facility in the United States that includes EMP protection. The building was a 2-story, 105 square-foot building, of which 44,000 square feet were EMP-protected, that included generators and cooling systems. The total project cost was about $100 million and the approximate EMP protection part of that was about $8 million. So if we're looking at it, about 8 percent of the overall budget. If we looked at that cost spread over the 2 million customers that that building serves, we're looking at less than a dollar per year, per customer spread out over 5 years.

While the optimum scenario is to protect a brand new control building, retrofitting is possible. I've spoken with quite a few electric utilities about retrofitting their control buildings. If we're looking at the existing facilities, they are tremendously vulnerable because the equipment was never intended to be EMP-protected, nor were the support systems ever laid out properly to be protected. An

estimated rough order of magnitude for protecting a similar facility as the 44,000 square feet that we talked about in the new building would be approximately $16 million. And there again, when you take a look at that and spread that out over 5 years, it's less than $2 per customer, based on the 2 million customer service area.

In my opinion, EMP protection of the electric utilities is the primary concern due to the survival and dependency we have on electrical power. Some proactive, forward-thinking utilities have either instituted EMP protection programs, or have at least begun to consider implementing them. However, the balance of the critical infrastructure segment, such as financial, wastewater, drinking water, transportation, food distribution, health care emergency services, have really not ever been addressed at all. It is my sincere belief that we as a Nation will some day face an EMP attack. I respectfully urge you to consider and pass legislation to address the EMP threat that I belive has been overlooked for far too long.

Chairman DeSantis, Chairman Lummis, ranking members, committee members, I thank you again for this opportunity to present my thoughts, and I would be very happy to answer any questions that you have of me. Thank you to your time.

[The prepared statement of Mr. Caruso follows:]

Subcommittee on National Security
Subcommittee on the Interior of the House Committee
On Oversight and Government Reform
Hearing on:
"The Threat: The State of Preparedness Against the Threat of an Electromagnetic Pulse (EMP) Event"
May 13, 2015

Good Afternoon, my name is Michael Caruso; I am Director of Government & Specialty Business Development for ETS-Lindgren Inc. ETS-Lindgren Inc. is the leading company that engineers and provides systems and components for the detection, measurement and management of electromagnetic, magnetic, and acoustic energy. Our roots date back to 1932 and we are globally recognized for our abilities to adapt new technologies and apply proven engineering principles in support of advanced technology projects.

I would like to thank Chairman DeSantis, Chairman Lummis, The Ranking Members and the Committee Members for this opportunity to testify at this hearing on EMP. I consider it an honor and a privilege to be here. I am here to share my 32 years of knowledge, experience and thoughts about the practical side of creating EMP protected environments.

For many years the U.S. Government and Military have addressed EMP protection for facilities and equipment that have been determined to be critical for National Defense. EMP hardening has been regarded as a very expensive and somewhat elusive art known to few. The current guidance document regarding EMP Protection is MIL-STD-188/125-1, Department of Defense Interface Facilities Performing Critical Time Urgent (Part 1 - Fixed C^4I Facilities) (17 July 1998). There are aspects of this specification, such as an all welded steel enclosure, that are overly restrictive and excessively costly for Critical Infrastructure non- C^4I applications.

In 2008, the EMP Commission, examined the evolving threat of EMP attacks on the United States and released a Critical National Infrastructures Report. The Report notes that government, public and private critical facilities and services are becoming increasingly interdependent. In addition to interdependency, those critical facilities and services are dependent on an increasingly vulnerable electrical power system. To date, little has been done to harden any of the 16 Critical Infrastructure Segments as designated by the Department of Homeland Security.

Eighteen states have ongoing initiatives to require electric utilities to address the protection of the electrical grid from the dangers of an EMP or a solar storm. Electromagnetic energy from an EMP can disrupt Supervisory Control and Data Acquisition (SCADA) systems on which the electrical grid relies. The States currently taking a proactive stand are: Alaska, Arizona, Florida, Kentucky, Maine, New Hampshire, New York, North Carolina, Colorado, Indiana, Louisiana, New Mexico Oklahoma, South Carolina, Texas, Utah, Virginia and Washington. I have recently testified at the Texas State House in support of Bills introduced by State Representative Tan Parker, State Representative Tony Tinderholt and State Senator Bob Hall. Texas is aggressively pursuing passage of EMP Legislation including a State appropriation to get Critical Infrastructure Segments started in the evaluation process.

To my knowledge, there are only three Electric Utilities in the U.S. that have taken steps in hardening their Operational Control Centers and Substation Control Buildings. I am prohibited by non-disclosure agreements, from directly identifying their names or locations. However, I can discuss the hardening process and costs of a recently completed facility.

Subcommittee on National Security
Subcommittee on the Interior of the House Committee
On Oversight and Government Reform
Hearing on:
"The Threat: The State of Preparedness Against the Threat of an Electromagnetic Pulse (EMP) Event"
May 13, 2015

In 2014, ETS-Lindgren was part of a multi-disciplinary team that successfully completed construction of the first large, private-sector SCADA facility in the United States that includes EMP protection.

The building is a new-construction, 2-Story 105,000 square foot concrete tilt-up building with:

- 44,000 square feet of EMP protected space
- Emergency generators and cooling systems protected
- Approximately 40 to 60 occupants in the protected space
- Approximately $50MM building construction cost (building only)
- Total project cost approximately $100MM (including equipment)
- Approximate EMP Protection cost $8MM (including additional subcontract costs)
- EMP protection was1-year on-site (concurrent with general construction)
- Average additional "total project costs" of 8% ($182.00/sqft)
- 2 million homes and businesses served
- 5,000 square-mile service area
- Less than $1.00 per year per customer (spread over 5-years)
- Performance certified by Little Mountain Test Facility (U.S. Air Force, Hill AFB)

While the optimum scenario is to include EMP protection in a new building, retrofitting existing buildings for EMP protection is somewhat more complicated and costly, but certainly achievable. I recently led a five-man team in an evaluation of two control centers (primary and back-up) for an electric utility in a major U.S. City. I am prohibited, by non-disclosure agreements, from directly identifying their names or locations.

As you might imagine, existing facilities have legacy equipment and systems that were never intended to be EMP protected. This condition makes these facilities tremendously vulnerable to EMP. The existing interconnecting wiring, conduits and mechanical systems provide excellent pathways to conduct the EMP directly to the critical equipment. Therefore, a comprehensive evaluation of the facility must first be conducted to identify the "must have" functionality and equipment in the case of an EMP event. As an example, in this case, it was determined that the large system display board did not have to remain operational because the individual operators would be able to see their sector status on their individual monitors. Therefore it was only necessary to address the protection of the individual stations and a cost savings could be realized. The most critical equipment must be grouped and isolated in individual interconnected enclosures to accommodate functionality. In addition, the existing back-up power systems, cooling systems and communication systems that support the critical equipment must be protected. In some cases this will involve creating new dedicated support systems due to the complexity of the existing systems.

Subcommittee on National Security
Subcommittee on the Interior of the House Committee
On Oversight and Government Reform
Hearing on:
"The Threat: The State of Preparedness Against the
Threat of an Electromagnetic Pulse (EMP) Event"
May 13, 2015

The estimated Rough Order of Magnitude (ROM) costs for retrofitting an existing facility of a similar size as the previously discussed new-building is:

- 44,000 square feet of EMP protected space
- Emergency generators and cooling systems protected
- Approximately 40 to 60 occupants in the protected space
- Approximately $10MM building construction cost (building only)
- Total project cost approximately $26MM (including equipment)
- Approximate EMP Protection cost $16MM (including additional subcontract costs)
- EMP protection 18 to 24 months on-site (concurrent with general construction)
- Average additional "total project costs" ($364.00/sqft)
- 2 million homes and businesses served
- 5,000 square-mile service area
- Less than $2.00 per year per customer (spread over 5-years)

While, in my opinion, EMP protection of electric utilities is the primary concern, due to the survival dependency we have on electrical power, all other segments of our nation's critical infrastructure must be addressed. Some proactive forward thinking electric utilities have either instituted EMP protection programs or have at least begun to consider implementing protection. However, critical infrastructure segments such as; financial, waste water, drinking water, transportation, food distribution, healthcare and emergency services have not.

It is my sincere belief that we, as a nation will someday, in the not too distant future, face an EMP attack. I have lectured and given workshops in both South Korea and Israel where they are certain that they will face an EMP attack and they are taking very active steps towards protection. I urge you to consider and pass legislation to address the EMP threat that I believe has been overlooked for far too long.

Chairman DeSantis, Chairman Lummis, Ranking Members and Committee Members I thank you again for this opportunity to present my thoughts and I would be very happy to answer any questions you might have of me.

Thank you for your time,

Michael A. Caruso

Mr. DESANTIS. I thank the witnesses for your testimony. The chair now recognizes himself for questions for 5 minutes.

Dr. Baker you talked in your written testimony about the critical importance of the electric grid. So an EMP attack that would fry the electric grid, can you just explain the consequences to somebody who maybe has never heard of an EMP before today's hearing, what practical effect would that have on American society?

Mr. BAKER. The electric grid is the foundation for all other infrastructures. DHS has listed 16 critical infrastructure sectors, and the one sector that every—depends, you know, that drives everything else is the electric power. The other thing about the electric power, it not only is the most critical, arguably the most critical infrastructure, it is arguably the most vulnerable to EMP because you measure EMP in volts per meter, so the longer the line, the larger the voltage it will be induced on the line.

So it's ironic that our most critical infrastructure is also the most vulnerable, and that's why we have to be so serious about protecting the grid. But without the electric grid, basic life services: The ability to pump drinking water, the ability to heat and cool our homes——

Mr. DESANTIS. Take our money from an ATM, would you be able to do that?

Mr. BAKER. Yeah, that's right. You would—you would—our financial sector is also way up there on in terms of EMP vulnerability and risk factor mainly because it depends upon the electric grid and the on call communications as well. So essentially it would be—we've seen sort of a microcosm of what could happen in the northeast blackout and the anarchy that resulted there, but that—in Britain, I've been to some EMP meetings in Britain, where they actually are protecting their grid—but their rule of thumb is it's 3 days to total anarchy, I heard this member of Parliament say—once you lose the electricity.

Mr. DESANTIS. And in terms of the some of the casualties, because people have surmised men, terrorists, if they can get their hands on a nuclear device, detonate an American city, obviously that would be very devastating. And someone said, yeah, that would be, but their best bet to do the most damage would be to try to launch it over the country and explode it and create an EMP. And the casualty estimates I've seen are really, really high if they were able to cripple our entire electrical grid. Is that your understanding that you are talking about potentially millions of people?

Mr. BAKER. That's my understanding. Even though you don't get direct effects on biological, humans—the long-term term effects without the electric power grid, we're talking about certainly within a year, you would lose at least half the American population. I have seen estimates as high as 90 percent of the American population would be at risk over a projected 1-year period.

Mr. DESANTIS. So given that the consequences are potentially very dire, but also given that, I think, as all the witnesses have said, there are certainly things we could do very easily, why haven't we done enough, in your opinion?

Mr. BAKER. One of the problems is that the liabilities, the public companies are reluctant to admit vulnerabilities, because if something bad were to happen, they would be liable, and I think that's

a big problem. And just the cost, the wide-area effects, we get into these hand-wringing stances where people—they don't know where to begin so they haven't. And what we're trying to do is lay out, you know, a well-ordered, incremental approach where to get us beyond the hand-wringing.

Mr. DESANTIS. Mr. Caruso, you've been involved in this field and have done work hardening critical infrastructure against an EMP attack. So help us understand what is involved when you actually try to harden a facility or a line?

Mr. CARUSO. Certainly. In addition to the critical infrastructure, I've been involved in hardening military and government facilities for the 32 years in this business. And essentially, what's required to harden a facility is to create an electromagnetic shield, a 6-sided electromagnetic shield around the equipment that's intended to be protected.

Mr. DESANTIS. As of right now, in your judgment, and based on your experience, what percentage of the electrical grid is prepared for an EMP threat?

Mr. CARUSO. Currently, there's only one control center in the entire country that I'm aware of that is protected.

Mr. DESANTIS. And which one is that?

Mr. CARUSO. I'm not allowed to say, because of non-disclosure agreements that I'm under.

Mr. DESANTIS. Understood. My time has expired. Thanks for answering the questions, and I now recognize the ranking member of the full committee—the subcommittee on National Security, Mr. Lynch, for 5 minutes.

Mr. LYNCH. Thank you, Mr. Chairman. So what we're saying here is that because of the interconnectivity of our society today, the great reliance and connectivity to the Internet, so much of every aspect of our lives is wired now, that that fact will actually amplify the impact of a EMP event. Is that basically what you're saying, Mr. Baker—Dr. Baker? Excuse me.

Mr. BAKER. That's right.

Mr. LYNCH. All right. Now, for countermeasures, I understand, and I don't question the level of disruption that would occur. And I guess the imminence of this is debatable, but there is no debate above the disruption that would result if one of these EMPs occurred. The countermeasures that have been talked about, the folks at CRS that serve Congress, the Congressional Research Service, mentioned a couple of countermeasures. One was this Faraday Cage protection, which I guess is some kind of a cladding. Can you talk about that for a bit?

Mr. BAKER. I can. Mike Caruso just mentioned the idea of a 6-sided shield. You have a six-sided metal enclosure, that's referred to in electrical engineering as a Faraday Cage.

Mr. LYNCH. Okay. Mr. Caruso, do you want to go into that a little bit more?

Mr. CARUSO. Certainly. The six-sided metal shield has to be constructed so it basically has no openings in it except those that are absolutely necessary to have. And all of those openings are technically considered to be points of entry. So you start out by building a six-sided metal box with no openings, and then you start adding openings for things like the electrical power, communications

and air exchanges and cooling systems. And all of those points of entries are handled in a very, very special and particular way in order to ensure that you are attenuating any EMP signal that might be broadcast in the atmosphere, but also any signals that are being brought in, conducted on the electrical lines or communication lines.

Mr. LYNCH. Sort of like a surge protector? That type of——

Mr. CARUSO. Exactly. A surge protector on steroids, if you would.

Mr. LYNCH. Yeah. Now, what about the other countermeasure that I'm not sure if it incorporates the Faraday Cage protection, these portable, or mobile units that, I guess, some of the contractors for Microsoft and, I guess, some of the other computer outfits have come up with, sort of an off-the-rack type of system where they can house all of these servers in the event that you have an event. Is that one and the same or are these two different strategies?

Mr. CARUSO. It's one and the same. In terms of technology, the portable data centers, if you will, the EMP-protected data centers are essentially six-sided Faraday cages with all the points of entry addressed, and sometimes they get actually interfaced with the fixed asset that might be inside of a building. So they become a supplement to what's going on in the building. These same shelters sometimes hold backup generator systems or backup cooling systems to act as protection against the EMP for those systems as well.

Mr. LYNCH. Okay. So the last time we had a talk about this, the study was done in 2008, I think, then there were 16 recommendations. Is there anything different that we're doing now than what was going on at that point, talking about Congress?

Mr. BAKER. The only substantive response to the EMP recommendations has been within the Department of Defense, where they are actually providing an annual report to Congress on the steps they are taking to meet the EMP Commission recommendations. But as far as the civilian infrastructure, I'm not aware of any progress.

Mr. LYNCH. Dr. Pry, I don't want you to get off the hook without a question. The general recommendation then would be to adopt some of these countermeasures for infrastructure that we identify as being critical, whether it's civilian critical infrastructure, or military infrastructure; is that right?

Mr. PRY. Yeah, that's right. You know, for example, there are 2,000 extra high voltage transformers that are basically the technological foundation of our electronic civilization, you know, most people don't even know that. These things are vulnerable to EMP. They should be protected. You know, they are very hard—we don't even make them in this country anymore. But that's an example of—the Commission had a rather long list of recommendations, basically a plan that could be implemented to protect the civilian critical infrastructure at affordable cost. It's not hard to do, the technology isn't the problem, the money isn't the problem, it doesn't cost that much to do it, it's the politics that has been the problem.

As George has said, nobody has responsibility for doing this, those who would think would have responsibility, the Department of Defense, for example. You know, when you talk about it, they

have no jurisdiction over the civilian critical infrastructure. And they will say, well, this could be caused by a geomagnetic storm and that's not our department. We are dealing with foreign threats, so it is the Department of Homeland Security's job. DHS will say, well, a nuclear weapon, that's the DOD's job, so nobody has been in charge.

And then where it counts the most is we have this very dysfunctional relationship between the NERC, the North American Electric Liability Corporation that represents the 3,000 utilities that is supposed to be—partner with U.S. FERC in providing for grid security. But the political reality is that that relationship is dysfunctional and it has not resulted in not only in increasing our security where EMP is concerned, but even against tree branch problems, for instance. It took NERC a decade to come up with a vegetation management plan to better manage tree branches so that we won't have a repeat of the great Northeast Blackout of 2003. They are falling down on job on very pedestrians threats, let alone cyber threats and EMP attacks and the like. It's just the system isn't working, and that needs to be fixed by somebody.

Mr. LYNCH. Thank you. I assume my time has expired. I yield back.

Mr. DESANTIS. The gentleman yields back. The chair now recognizes the gentlewoman from Wyoming, the chairman of Natural Resources Subcommittee for 5 minutes.

Mrs. LUMMIS. Thank you, Mr. Chairman. I'm a bit of a novice to this subject, so I'm going to ask you some general questions, feel free to take them wherever you choose. You know, over the weekend I got a little taste of this. I woke up Sunday morning in my country home, in Wyoming, without electricity. I had no water because in a rural area I'm on an electric pump to pump my well water. So the inconveniences associated to being without electricity were apparent from the minute my eyes opened.

As it turned out, it was just something, I think they called it a bayonet which is a very large fuse that they just came and replaced. And believe it or not, they came on Sunday morning and I was back up and running, and happily so. But when you think about that on the scale that we're talking about, it really does create immediate global problems, especially in this country.

So my first question, Mr. Caruso, what do these things cost, these shields that protect our infrastructure?

Mr. CARUSO. The shield that I gave an example of in my testimony was approximately $182 per square foot to put into place. So if you look at a floor plan of a building and look at the square footage, again, about $182 a square foot on top of the building cost itself.

Mrs. LUMMIS. So it's not chump change.

Mr. CARUSO. It's not chump change, but it's not insurmountable either.

Mrs. LUMMIS. My next question is for all of you. I am going to direct to Dr. Pry first, but then I'd like to ask our other two witnesses to weigh in. This is about your concern that the relationship between NERC and FERC is dysfunctional. You mention the possibility of doing away with both. So if you were dictator for a day, and you could do exactly that, either combine NERC and FERC or

do away with them and replace them with something else that would solve the dysfunction you've identified, as well as address this electromagnetic pulse issue responsibly, what would that look like?

Mr. PRY. That would look like the kind of relationship that the Federal Aviation Administration has with the air line industry. What I think that isn't understood is that the electric power industry is the only critical infrastructure that still operates basically in something that's close to a 19th century regulatory environment. The Federal Aviation Administration has the power and has independent inspectors. If they find metal fatigue in the wings of an airline, they can ground that whole fleet and order the air line industry, you are not going to fly those planes until they are fixed.

When there is a disaster and an airplane crashes, the industry doesn't get to investigate and figure out what went wrong, not by themselves. It's the Federal Aviation Administration that drags those things into a hangar. And why do we do that? Because we want an objective actor whose first priority is public safety, because hundreds of lives are at stake when airplanes fly and so we don't—you know, we don't take lightly, you know, the lives of the American people when it comes to that. If we go to the Food and Drug Administration or any other industry, I would like that same kind of regulatory relationship with the electric power industry.

Let me describe to you a little bit about what the current regulatory environment is like, because it's not really what we would consider a regulatory environment. The U.S. FERC, for example, does not have the power to tell NERC, that is, the industry, what they shall do to protect the grid. It can order them to come up with a plan and then NERC can take as much time as it likes to come up with a plan or a proposed plan. And then if the U.S. FERC has objections that plan, the whole plan has to be scrapped, and the process starts all over again.

That's how it took 10 years to get a plan for vegetation management, you know, so we wouldn't have a repeat of the great Northeast Blackout of 2003. Industry takes its time dragging its feet and can use the process, you know, to basically escape doing what it's supposed to do. The NERC is supposed to partner with the U.S. FERC in providing for the security of the American people, but it doesn't. And I don't think combining these or keeping the same—I mean, there are some good people in these institutions, but George and I have served, for example, on the NERC's Geomagnetic Disturbance Task Force, and we have actually seen them engage in junk science, dishonest practices, you know, in terms of the science to try to mislead people.

In my written testimony, I describe a very disturbing example of where the NERC came up with a hollow standard for the natural EMP created by the sun saying, okay—they were dragged, kicking and streaming by the way and resisted for years saying that oh, the threat from the sun doesn't really affect the electric grid, which was completely untrue. Eventually they were forced to come up with a standard, the standard is so low, that it doesn't provide any real protection.

Mrs. LUMMIS. Dr. Pry, my time has expired, but I'm hoping to follow up with all three of you on this issue in a second round of questioning. Thank you all very much.

Mr. Chairman, I yield back.

Mr. DESANTIS. The gentlelady yields back. I ask unanimous consent to enter into the record a statement of Ms. Lawrence, who is the ranking member on the Subcommittee on Interior. Without objection, that will be so ordered.

Mr. DESANTIS. At this point, I would like to recognize Mrs. Lawrence for 5 minutes for her questions.

Mrs. LAWRENCE. Thank you, Mr. Chairman. We—this issue is one of great importance to me and to our country. The congressional EMP Commission issued a report in 2008 identifying 16 segments of our infrastructure that could suffer severe damage if not protected. Today, 7 years later, the testimony continues to echo those concerns. I'm curious today, Mr. Caruso, has anything changed since this last report regarding the protection of the grid?

Mr. CARUSO. I don't believe anything significant has changed. What we have seen is that many private industries that make up the critical infrastructure have taken it upon themselves just as doing good business to do EMP protection. I have worked with several financial institutions, including insurance companies. I've worked with electric utilities and have done some work counseling, the gas and electric industry as well, but other than that, nothing real significant has happened.

Mrs. LAWRENCE. To follow up on your statement, there has been some independent efforts being made in this direction. Are we monitoring that as a Federal Government if we start implementing the—taking the steps that we should, would we have a different system that is being used now, or are we just going to provide oversight to these individual companies? What is the plan that you're recommending here?

Mr. CARUSO. My recommendation really falls in line with those of Dr. Pry and Dr. Baker in that someone needs to be in charge, and especially as it's related to the 16 critical infrastructure segments in terms of providing real protection, and at least addressing the issue to ask the question what if, what happens if we lose the electrical power? What happens if we lose the ability to do it? I use—I like to use the example of the waste treatment systems. You would not only lose the electrical power, but the control systems that control the wastewater filtration and pumping stations throughout an area. If that goes down in a major city, you have 2 or 3 days before the city is just on its knees.

Mrs. LAWRENCE. My question is to Dr. Baker. As we look at the need, we heard your recommendations, 2008 was the last report. Will we have to initiate a new commission and a new report so it would be relevant, or do you feel strongly that the information we have now is enough to move forward with starting our plan?

Mr. BAKER. I believe that the EMP Commission reports that were issued in 2004, 2008 are still operative, and so I would say yeah, they are a very good place to start. I don't know whether there is anything I can add to those reports. The thing that helps us is that—I understand that there's going to be a lot of new construction on the electric grid, and that if we are able to project and

develop some plans that we can actually include EMP protection with the new build-out. So there might be some maybe augmentation of the EMP Commission recommendations.

Mrs. LAWRENCE. I do want to say as my time runs out that as a mayor, I lived through the power outages that affected the Midwest. And when you talk about the threat of lives, hospitals that were in my city, individuals stranded on elevators, life support systems and oxygen, getting the pumps backed up with batteries so that we could continue to ensure that our water was properly processed through cleaning water filtration, this is a very serious issue. And I appreciate your testimonies today, and I know for a fact if we receive such an attack, the threat is one that would be significantly dangerous for our country and a lot of dangerous people on simple mere traffic navigation, everything came to a complete halt. To be able to sit in a room in our emergency command center with no power, we could not pull up documents of employee records, because it was on a computer. So it taught me a lot of how we were dependent just from being a mayor and trying to manage through that power outage. So I thank you today for your testimony.

Mr. DESANTIS. The gentlelady's time has expired.

The chair now recognizes the gentleman from Georgia for 5 minutes for his questions.

Mr. HICE. Thank you.

Dr. Pry, what Federal agency do you believe is best suited to lead a preparedness effort for this? Is it Homeland Security? Is it Energy? Which one is it?

Mr. PRY. I think the Department of Homeland Security, that it naturally falls under their jurisdiction, you know, because they're responsible—they're supposed to be responsible for critical infrastructure protection in the first place. So I think that they're the ones.

However, DHS and the Department of Defense are also supposed to have a cooperative relationship, you know, when it comes to providing for homeland security. There's a lot of expertise—now, DHS should have the lead, but there's a lot of expertise in the Department of Defense. And the Department of Defense is also dependent on the civilian critical infrastructure.

Mr. HICE. All right. But, at the end of the day, DHS, you believe.

Mr. PRY. I would say DHS. I'd like——

Mr. HICE. All right.

Does DHS currently have anything to deal with the scenario—they've got the 15 national planning contingency scenarios. Is anything dealing with EMPs a part of those 15 plans?

Mr. PRY. No, they're not. And that's part of the problem and why we need to pass the Critical Infrastructure Protection Act.

And I would add that there are people—there are people within DHS that are standing by, waiting for us to do exactly that. The——

Mr. HICE. All right. So there needs to be—if DHS is responsible, DHS then needs some sort of plan. Is there a reason there is not a plan, if DHS is responsible?

Mr. PRY. The—I think the—I don't know what the motive has been within the leadership of DHS, because it's been a bipartisan failure, you know——

Mr. HICE. But a failure it is. We don't need to elaborate. If DHS is responsible, that is one thing. If DHS is responsible and not prepared, that is another issue that certainly needs to be addressed.

Mr. PRY. I'd say they are responsible and not prepared.

Mr. HICE. Okay. Well, then we have to—that definitely needs to be addressed.

Let me go, Mr. Caruso, to you. Hardening a facility, can you elaborate a little bit more on just what that means and what it involves?

Mr. CARUSO. Certainly.

As was mentioned before, we're talking—the scientific term is "Faraday cage." And it essentially—we use steel to do that. So it encloses the area that's intended to be protected in a six-sided steel enclosure. And all of the points of entry coming in and, most importantly, the electrical power are fitted with filter devices and suppression devices that would suppress an EMP coming down the line being conducted in from the external power lines.

In addition to that, the facility shield protects all of the equipment inside from the radiated effects of an EMP coming down out of the atmosphere. And it needs to also protect the backup generators, the cooling systems, and all of the other support systems that would support a facility.

Mr. HICE. Okay. I just have a couple minutes, so that—just a general understanding, I appreciate what you just shared.

Do State governments—and I will just keep this with you, Mr. Caruso—do State governments have anything right now to protect against EMPs?

Mr. CARUSO. Absolutely nothing.

Mr. HICE. Nothing. All right. So we are totally vulnerable. That includes all 50 States; there is nothing out there?

Mr. CARUSO. Nothing that I'm aware of.

Mr. HICE. All right. All right. So we have got to address this problem because it is totally not addressed anywhere.

Mr. CARUSO. That's correct, except for a handful of private industry actors that have taken it upon themselves to protect it. The control center that I was speaking of before is an electric utility. They took it upon themselves to invest their own money to protect their control center.

Mr. HICE. Okay. Then, real quickly, across the board, and I would appreciate an answer real quickly from all three of you. This being the case, what steps do Federal entities need to take to protect this?

And, Dr. Baker, I will start with you, just real quickly because I know my name is about up.

Mr. BAKER. First, we need a single authority that is in charge with the power to develop and enforce requirements.

Mr. HICE. Okay.

Mr. BAKER. And then I think, you know, of the 16 critical infrastructures, if we focused only on the electric power grid, that would be well worth it. We should have a program to——

Mr. HICE. All right.

Mr. BAKER. —protect the grid.

Mr. HICE. Real quickly, Dr. Pry and Mr. Caruso?

Mr. PRY. Pass the Critical Infrastructure Protection Act, which will require the Department of Homeland Security to add a new national planning scenario focused on the EMP threat. All State, local, and Federal emergency planning, training, and resource allocation is based on those scenarios. That's why it's not on the radar screen right now. Bring back the congressional EMP commission so you can have an aggressive watchdog to make sure that this work gets done.

And reform the dysfunctional relationship between NERC and FERC. I say abolish them and start all over again. Give the job to DHS, somebody that's willing to do the job.

Mr. HICE. Unfortunately, my time has expired, but could Mr. Caruso——

Mr. DESANTIS. If you can submit your response——

Mr. HICE. Thank you.

Mr. DESANTIS. —for the record written, it would be great.

Mr. HICE. Thank you, Mr. Chairman.

Mr. DESANTIS. And the chair now recognizes the gentleman from California, Mr. Lieu, for 5 minutes.

Mr. LIEU. Thank you. Thank you, Mr. Chair, for holding this hearing to inform the public and policymakers about the threat of an EMP device.

I have just some preliminary questions. Let's say an EMP device was exploded over the U.S. What is the geographic area that it would affect? Is it the size of D.C.? Of Maryland? Of Virginia? Smaller? Larger?

Mr. BAKER. An entry-level, you know, low-yield weapon, if it's detonated at the optimum altitude, the diameter of the effect would be 1,200 miles. So it would be a circle with a 1,200-mile diameter.

Mr. LIEU. Okay.

And then, within that circle—so let's say it fries the electrical generators. Does it also destroy the lines themselves, or are they still fine?

Mr. BAKER. The——

Mr. LIEU. The lines that connect houses and businesses to the electric grid.

Mr. BAKER. The lines will remain intact. There was some Russian experience where some of their lines, they actually had damage to the support insulators, where some of their lines fell to the ground. But the evidence is that, in most cases, the lines would remain intact. It's just what's on the end of the line would be affected.

Mr. LIEU. And then, based on the way our electrical power grid is constructed in the U.S., could you take power from another part of the country and route it through the affected area?

Mr. BAKER. That would depend upon the size of the circular diameter. It would be difficult to do that because you're looking at areas that are crossing, you know, State boundaries and the boundaries of the different power companies. So it could be difficult.

And we don't—the grid control centers—we don't have grid control centers in most cases that span that large of an area.

Mr. LIEU. Okay.

And I think, Mr. Caruso, you had mentioned a cost to harden our critical infrastructure. You said $182 per—per what?

Mr. CARUSO. Per square foot of floor space.

Mr. LIEU. Okay.

Mr. CARUSO. And that's for doing a facility, not looking at the transformers.

Mr. LIEU. So it's hard for me to understand what that means. Can you sort of give me a number? To harden the United States to a place you think is sufficient, are we talking about $50 million, $50 billion, $500 billion? What is the range here so I can understand that?

Mr. CARUSO. I'm sorry, I really don't have that number available in my head. I can submit something.

Mr. LIEU. Sure.

Or anyone on the panel?

Mr. PRY. It depends on how much protection you want to buy and what your judgment is, okay? It's sort of like asking, well, how much will it cost to buy fire protection for my house? You know, some plans can be very inexpensive. It can be as simple as buying a smoke alarm—okay?—you know, which would cost you very little. Others might want to put a fire extinguisher in every room and put a sprinkler system in, which is going to cost a lot.

There are—here are some legitimate plans and legitimate prices for you to keep in mind—okay?—that can range—John Kappenman, who was on our commission, had an idea, a plan, that would cost $200 million. And the idea here would be to protect the 200 most important extra-high-voltage transformers, the ones that service the major metropolitan areas. So John wouldn't say that this is adequate, but it will at least give you a fighting chance to save millions of people from starving to death, you know, because the transformers, at least, would be saved.

The EMP Commission had a plan. It's, you know, right in the plan, it's about $2 billion—okay?—that protects all of the transformers and generators and is much more ambitious. And, you know, that's a much better plan and would give you much greater resiliency and confidence in being able to recover the society quickly from an EMP.

George Baker described an even better—a more ambitious and, I would say, a better plan that goes beyond that. It sort of depends on how much do you want to put into prevention. Just like in protecting your house, you know, you can spend more money to protect your house and be safer, or you can decide to spend less money and be less safe.

But there are a wide variety of plans, which——

Mr. LIEU. And——

Mr. PRY. —industry sometimes misrepresents as being contradictory. They're not. You know, it could range from $200 million up to $20 billion, $30 billion.

Mr. LIEU. And so, given those options—as you know, a lot of electrical utilities are regulated by States or cities. What is your view of the Federal Government's role? Why is it we don't leave it up, for example, to the Public Utilities Commission of California to decide if they want to increase fees on ratepayers in order to harden the facilities there?

In other words—or is it your view we should give DHS authority to simply start imposing additional costs on ratepayers so we can harden all these facilities?

Mr. PRY. May I respond?

Mr. LIEU. Yeah, of course.

Mr. PRY. Yeah. Well, you know, because this is—ultimately, this is a national security—especially if you're talking about a nuclear EMP attack or a great geomagnetic storm that could cover not just the United States, but if it's a Carrington event, you're talking about the entire world being affected by this kind of a phenomenon.

A threat of this scale should be a Federal national security responsibility. The States don't normally think of themselves as protecting themselves against nuclear terrorist attacks, but because of the——

Mr. LIEU. But they do think about—right?—natural disasters. I mean, a massive naturally caused EMP thing would be a natural disaster. So, in California, it's not so much the Federal Government saying, "Hey, harden yourself against earthquakes." It's actually California building codes that do that.

So I'm just sort of curious as to, do you want this massive, overreaching Federal plan, or should we leave it to States and cities and local control?

Mr. PRY. I personally don't think it should be left to States and cities. But, however, you're getting your wish. Because of the vacuum that's been created by the lack of Federal leadership on this issue, the States are taking the initiative because they have to.

Next week, I'm going up to Maine because Maine has passed a bill to protect its electric grid because the Feds haven't done anything. Virginia has passed a bill. Arizona has passed a bill to protect its people. Florida has established a cyber and EMP legislative working group because there is no leadership, no help coming from Washington.

And so the States are being made aware. They don't even know about this threat, most of them, but as they become aware of this threat and they realize that the Federal Government isn't doing anything, they are stepping up to the plate to protect their people.

I don't think that that's—I was originally trained as a historian, and I find that rather disturbing, the fact that the States have to do this. You know, in the—one of the signs of the decline and fall of the Roman Empire was the rise of walled cities, because Rome would no longer—could no longer defend its cities against the Barbarians. So the states had to start providing for their own—I mean, the cities had to start providing for their own security.

I don't think that's the way our system is supposed to work. You know, when it comes to national security, the Feds aren't supposed to just say, "Well, the States, go ahead and do the best you can to take care of yourselves. We've got other things to do here." You know, the fundamental constitutional obligation, the reason we have a Federal Government, is to provide for the common defense.

Mr. LIEU. Thank you.

Mr. DESANTIS. The gentleman's time has expired.

The chair now recognizes the gentleman from Tennessee for 5 minutes for his questions.

Mr. DUNCAN. Well, thank you very much, Mr. Chairman. And thank you for calling this very important hearing.

This is just one of thousands of things that we deal with, so none of us are the experts that you all are, but I can tell you this, it's something I've been concerned about for a long time.

In fact, just a few days after the 2003 blackout, I gave a speech on the floor, and I quoted from the Associated Press story at the time. And it said the proposed improvements that they were talking about to keep this from happening a second time, it says, "are making the electricity supply vulnerable to a different kind of peril—computer viruses and hackers that could blackout substations, cities, or entire States."

And the story went on to say, it said, "In the past, the grid's old electromechanical switches and analog technology made it more or less impervious to computer maladies, but now switches and monitoring gear can be upgraded and programmed remotely with software, and that requires a vulnerable connection to a computer network. If that network runs on Microsoft Corporation operating systems, which virus writers favor, or it connects to the Internet, the vulnerabilities are increased."

That's what came out in 2003. And I'm sorry that I've had to run in and out of here and not hear everything you've said because I've had some meetings with constituents. But when I hear you talking about knocking out the power to 80 percent of Turkey—somebody mentioned that—and all of Yemen, in some ways it seems like we're almost more vulnerable today than we were then. Are we?

Mr. BAKER. The quick answer is "yes."

Mr. DUNCAN. Well, you know, my wife has told me for years I still live in Andy of Mayberry days. And then, a few years later, I saw that I had the same birthday as Don Knotts. And when I saw that, I thought, well, she's been right all these years. So I'm about as low-tech as they come.

But it seems ridiculous to me that we're so interconnected with each other that, when a crew cuts a tree limb in Cleveland, Ohio, and it cuts off the power to the entire Northeast and part of Canada for several hours, I mean, it seems like, to me, that that's just ridiculous that we would allow that to happen.

And it also seems to me that we need to get more people interested in this. Because surely we have people that can figure out—is it possible, you know, that bigger may not always be better? That maybe we shouldn't have these power companies that are so big that, if we broke up some of these power companies, that we wouldn't be so interconnected, where what happened to one would affect people all over the country?

Mr. PRY. Well, actually, that was one of the recommendations of the EMP Commission. It's called "islanding."

And, in effect, it's kind of what's happening at the level of the States. Even though it isn't happening by a plan coming out of Washington, by this natural process of the States deciding to protect themselves, you're creating islands, you know, where, if the big grid goes down, at least that State will have its lights stay on. And so——

Mr. DUNCAN. Well, that is encouraging. I've been glad to hear that, that some of these States are taking individual initiatives. I hope that keeps growing.

Mr. PRY. It makes it harder to do when the NERC claims that they've adopted a GMD standard and don't worry about it, they're on top of the problem, which they also say about cyber and things like that, which tends—is not true, you know, because it ends up taking away the incentive for the States to protect themselves when NERC convinces them that they are.

And one—I'd like to also make one last statement, because you talked about, are we getting more vulnerable? Another thing that needs to be kept in mind is that we are getting more vulnerable all the time because of the advance of technology. You know, as our semiconductor technology gets better and better and faster and faster and runs on lower and lower voltages, it becomes more and more vulnerable to the EMP effect, which is why we're so vulnerable now.

Back in 1962, Starfish Prime test, when that happened, the vacuum tube technology of the day, you know, was 1 million times less vulnerable to EMP. Still, the lights went out in Hawaii—1 million times less vulnerable.

And every time—I think it's every 10 years we have, like, a tenfold increase in the capabilities of our semiconductor technology. It also becomes tenfold more vulnerable to EMP. So this problem is getting worse and worse. It's not just standing still while we do nothing.

Mr. DUNCAN. Well, what do you think about this bill by Congressman Franks? Is that a good first step?

Mr. PRY. Oh, the Critical Infrastructure Protection Act? Absolutely. It's, you know—it would go in a huge way toward helping solve the problem.

Mr. DUNCAN. I remember several years ago I read on the front page of The Washington Post one day that a 12-year-old boy opened up the floodgates at the Hoover Dam 700 miles from his home because he was able to hack in. And it seems to me that, you know, we have a lot of brilliant people out here that should be able to—that should be working on this.

We oversensationalize a lot of these threats because of a 24-hour news cycle and because so many people in companies make money off of threats that are exaggerated. But, in my opinion, this is one that's not being exaggerated and that we need to do a little bit more. And I appreciate what you all are trying to do.

I've run out of time. I'm sorry, Mr. Chairman. Thank you.

Mr. DESANTIS. The gentleman yields back.

I want to thank the witnesses for their testimony, for answering our questions.

We wanted to have Congressman Franks testify and present both his critical infrastructure bill and the SHIELD Act, but he has a bill on the House floor right now, and he's not able to attend. So we're sorry that that couldn't be arranged.

But, clearly, I think, from what the witnesses have said, you know, those are the types of pieces of legislation, you know, that I think we need to be moving ahead in Congress. And so, if this

hearing has helped raise more awareness—and hopefully we can get some bipartisan support for this stuff and move forward.

I will hold the record open for 5 legislative days for any members who would like to submit a written statement.

Mr. DESANTIS. And, with that, this hearing is now adjourned.

[Whereupon, at 3:40 p.m., the subcommittees were adjourned.]

APPENDIX

Material Submitted for the Hearing Record

"Identify Potential Impacts of an Electromagnetic Pulse (EMP) Attack on Fire and EMS Delivery Services for the Walpole Fire Department" by Deputy Chief Michael K. Lararacy, Sr., Walpole Fire Department, Walpole, Massachusetts, can be found here: *http://www.usfa.fema.gov/pdf/efop/efo46308.pdf*

Submission of William R. Graham

Chairman of the Commission to Assess the Threat to the United States from

Electromagnetic Pulse (EMP) Attack

To the Committee on Oversight and Government Reform

U.S. House of Representatives

The EMP Commission was established by the Congress of the United States in Public Law 106-398, Title XIV, which stated:

SEC. 1402. DUTIES OF COMMISSION

(a) Review of EMP Threat. The Commission shall assess:

(1) the nature and magnitude of potential high-altitude EMP threats to the United States from all potentially hostile states or non-state actors that have or could acquire nuclear weapons and ballistic missiles enabling them to perform a high-altitude EMP attack against the United States within the next 15 years;

(2) the vulnerability of United States military and especially civilian systems to an EMP attack, giving special attention to vulnerability of the civilian infrastructure as a matter of emergency preparedness;

(3) the capability of the United States to repair and recover from damage inflicted on United States military and civilian systems by an EMP attack; and

(4) the feasibility and cost of hardening select military and civilian systems against EMP attack.

(b) Recommendation. The Commission shall recommend any steps it believes should be taken by the United States to better protect its military and civilian systems from EMP attack.

The Commission issued two reports:

Volume I : Executive Report, issued in 2004, and

Critical National Infrastructure, issued in 2008.

Both of these reports are available at http://www.empcommission.org/reports.php

SUMMARY AND CONCLUSIONS:

The Commission concluded:

Several potential adversaries have or can acquire the capability to attack the United States with a high-altitude nuclear weapon-generated electromagnetic pulse (EMP). A determined adversary can achieve an EMP attack capability without having a high level of sophistication.

EMP is one of a small number of threats that can hold our society at risk of catastrophic consequences. EMP will cover the wide geographic region within line of sight to the nuclear weapon. It has the capability to produce significant damage to critical infrastructures and thus to the very fabric of US society, as well as to the ability of the US and Western nations to project influence and military power.

The common element that can produce such an impact from EMP is primarily electronics, so pervasive in all aspects of our society and military, coupled through critical infrastructures. Our vulnerability is increasing daily as our use of and dependence on electronics continues to grow. The impact of EMP is asymmetric in relation to potential protagonists who are not as dependent on modern electronics.

The current vulnerability of our critical infrastructures can both invite and reward attack if not corrected. Correction is feasible and well within the Nation's means and resources to accomplish.

RECOMMENDATIONS:

The damage level could be sufficient to be catastrophic to the Nation, and our current vulnerability invites attack. The scale of the problem encompasses the electrical grids of the entire North American continent, and therefore requires careful planning, prioritization, and implementation to be carried out in a timely, effective, and affordable manner. It is possible to achieve an acceptable level of risk by reducing the invitation to EMP attack that follows from our current level of vulnerability, and to survive should we be attacked, with a strategy of:

- Pursuing intelligence, interdiction, protection, and defense to discourage, and if deterrence fails, to survive EMP attack against the US and its interests;
- Protecting critical components of the infrastructure, with particular emphasis on those that, if damaged, would require long periods of time to repair or replace;
- Maintaining the capability to monitor and evaluate the condition of critical infrastructures;
- Recognizing an EMP attack and understanding how its effects differ from other forms of infrastructure disruption and damage;
- Planning to carry out a systematic recovery of critical infrastructures;
- Training, evaluating, "Red Teaming," and periodically reporting to the Congress;
- Defining the Federal Government's responsibility and authority to act;
- Recognizing the opportunities for shared benefits;
- Conducting research to better understand infrastructure system effects and developing cost-effective solutions to manage these effects;

The cost for such improved security in the next three to five years is modest by any standard—and extremely so in relation to both the war on terror and the value of the national infrastructures involved. Costs at later times may be adjusted to deal with the then-apparent threat and future levels of effort required.

Finally, it is also essential to recognize that EMP is not an isolated threat. Today and for the foreseeable future, widespread threats also exist for cyber attack, geomagnetic storms, and physical assault on our national infrastructures and in particular the national power grids, which energize our other critical infrastructures. Intelligence, interdiction, protection, and defense of our national infrastructures should address all of these threats in an integrated manner to be both effective and affordable.

####

Biographical Note on William R. Graham

William R. Graham received a Bachelor of Science Degree in physics with Honors from the California Institute of Technology in 1959, and a PhD. in electrical engineering from Stanford University in 1963. In additional to working in the aerospace industry to protect U.S. strategic deterrent systems, he served as an officer in the U.S. Air Force, Deputy Administrator of NASA, Director of the Office of Science and Technology Policy in the Executive Office of the President, and Science Advisor to Presidents Reagan and his immediate successor, President Bush. Dr. Graham retired in 2005 and lives in San Marino, California.

Submission of William A. Radasky
President and Managing Engineer, Metatech Corporation

To the Committee on Oversight and Government Reform
U.S. House of Representatives

Background

I started my career as a 2nd Lt. in the U.S. Air Force in 1968, as a research engineer stationed at Kirtland AFB, New Mexico. In my 4 years of service there, I had the opportunity to work in the EMP Branch of the Air Force Weapons Laboratory (AFWL). In 1972 I left the service to join a private firm performing research for the U.S. Government dealing with the threat of EMP on military systems. Since that time I have worked continuously on this threat transitioning in the early 1990s to evaluate the effects of the high-altitude EMP (HEMP) on the civil infrastructures.

To avoid confusion I should mention that EMP is a general term used in the military and in scientific areas of research as the electromagnetic pulse created by a nuclear explosion at any altitude. The nature of the waveform (and its magnitude) changes drastically when a burst is close to the ground, as the peak fields decrease rapidly with range from the burst. For a burst in space (above 30 km) we refer to this type of EMP as HEMP, and it covers an enormous area (continental scale). It is thus the most important type of EMP for ground-based infrastructure systems. For that reason I will use the term HEMP in my testimony.

During the atmospheric nuclear testing program, the United States detonated a series of high-altitude bursts over Johnston Island in the North Pacific in 1962 to study the impacts on communications and to understand any other effects that might occur. This was known as the Fishbowl Series with the Starfish Event as the most publicized test of the series. Starfish created some effects in Honolulu (some streetlights were turned off and fuses had to be manually replaced) from the 400-km burst altitude 1400 km from Honolulu. There were other effects on the ground (but not spectacular in nature); fortunately scientists were able to measure the HEMP fields produced by Starfish and the other tests. Over the following years Drs. Bill Karzas and Conrad Longmire were able to establish the basic theory of the initial portion of the HEMP (using the measured data), and later Dr. Carl Baum at AFWL designed a series of large HEMP simulators to enable the testing of military systems (missiles, aircraft, etc.) to these fields. Others, including Dr. William Graham, worked on protecting against the threat of ground burst EMP to our missile silo systems. In the late 1960s digital computers were fast enough to allow computer codes to compute the HEMP fields for different scenarios, and I was able to perform the first code/data HEMP comparisons for the Fishbowl series of tests.

As the electronics in military systems became more sophisticated in the years after 1962 and as they transitioned from analog to digital in nature, there were more HEMP impacts noted during testing that required "hardening" of these systems. This trend has continued to today, as solid-state commercial electronics are more sensitive than ever to electromagnetic interference. In order to make the hardening of systems more efficient, the military developed HEMP standards to make the process more repeatable and efficient.

After the end of the cold war, we have observed the proliferation of nuclear weapons (and long range missiles) throughout the world and the rise of terrorism, so now there is a concern that a single HEMP burst could cause massive problems to our commercial infrastructures, including the national power system, our communications systems, financial systems, and many others. While all of the infrastructures are critical in the

end, studies performed for the EMP Commission and published in 2004 and 2008 clearly indicate that the power system is the "keystone", and that the other infrastructures will quickly fail without power. For this reason I will emphasize the power system infrastructure in the rest of my testimony.

Studies of the U.S. Power System for HEMP

During the early 1990s my company, Metatech Corporation, began to study the impact of geomagnetic storms on the high voltage (bulk) power grids in the United States and in other countries in Europe and Asia. This was a reaction to the large blackout caused by a severe geomagnetic storm in the Province of Quebec in March 1989 that occurred due to the arrival at the Earth of solar charged particles generated in a coronal mass ejection (CME). Our assessments indicated that many power grids were vulnerable to this threat and that power companies should consider both operational and hardening approaches to make themselves less vulnerable to this problem.

At the same time I began to work as a volunteer to the International Electrotechnical Commission (IEC) in Geneva, Switzerland to develop standards for commercial systems to survive both the early-time E1 HEMP (first microsecond) and the late-time E3 HEMP (after 1 second). The late-time E3 HEMP waveform is similar to the fields generated on the Earth by a severe geomagnetic storm, hence the strong connection between research and standards in these two apparently unrelated areas. The HEMP work in the IEC was fully integrated with the commercial standardization of electromagnetic compatibility (EMC), which ensures that modern electronics (like personal computers) are not damaged by electrostatic discharge or by the fields from nearby cellular phones. I have had the privilege to chair IEC SC 77C since its inception in 1992 to the present. We have produced 21 standards and other publications dealing with the protection of commercial electronics from HEMP and other high power electromagnetic threats.

In 2001 the EMP Commission contracted with Metatech to evaluate the effects of E1 HEMP and E3 HEMP on the U.S. power system. Over several years of work, we purchased electronics used by power companies in critical operations in their high-voltage substations, their bulk grid control centers and in power plants. For low-voltage electronics, we tested them to damage to determine their susceptibility levels and then we performed validated analyses to determine the level of induced transients that could be propagated to the electronics. This comparison provides insight into the vulnerability of the electronics. In addition we examined the performance of power line insulators on distribution power lines and the stability of high-voltage power grids due to the E3 part of the HEMP. Due to the similarity of E3 HEMP to the severe geomagnetic storm threat, we also evaluated the impact of significant geomagnetic storms on the U.S. power grids. Our results indicated that there was a significant likelihood of long lasting blackouts due to both the E1 HEMP and the E3 HEMP on the power networks. This information was provided to the EMP Commission for their evaluation. It should be noted that the Metatech approach to this work and some of the details of our experiments and analyses were peer reviewed over the years in scientific publications.

After the work of the EMP Commission was completed, we were asked by the Federal Energy Regulatory Commission (FERC) to publish a series of reports summarizing the severe electromagnetic threats to the power grid and the options for protection, and these reports were produced for Oak Ridge National Laboratory and are listed at the end of this statement.

Response of the Power Industry

After the end of the EMP Commission work, we performed electromagnetic assessments for a number of large power companies in the United States. These assessments included studies of the vulnerabilities of their substations, their control centers and their high voltage grid (including their transformers) to HEMP, IEMI and severe geomagnetic storms. In two cases power companies decided to harden new power control centers against the E1 HEMP and also electromagnetic weapons that could produce Intentional Electromagnetic Interference (IEMI). The IEMI threat waveforms are very similar to E1 HEMP, but IEMI is a local security threat illuminating typically one "target" at a time. I have listed some references and standards at the end of this statement covering this threat (it was also covered in the work we performed for FERC).

During the construction project of an E1 HEMP-protected control center, it was possible to produce a shielded building at low cost. This was not unexpected, as the military has stated from its years of experience that building a new facility with an electromagnetic shield integrated into the structure usually costs an additional 3-5 % of the cost of the entire facility (building plus its contents). There are other power company projects currently underway, including a retrofit hardening project, so industry is moving forward on its own.

Unfortunately there is a problem that other large power companies are not being encouraged to move forward with protection. After early support from NERC and FERC to discuss these threats and protective solutions, it seems that their attitude is now that these threats are not likely enough to consider. While it is agreed that the probability of an attack does not seem very high, the impact of such an attack could be devastating. This was precisely one of the points raised by the EMP Commission in their reports. The Commission also stated that the lack of action concerning a known vulnerability can invite an attack.

Recommendations

Based on my 47-year career studying severe EM disturbances and my strong experience in dealing with the protection of commercial systems from severe electromagnetic disturbances, I feel that action from the Congress at this time is very important. I recommend the following activities:

1. The EMP Commission, or a similar group of highly qualified individuals, should be reconstituted with the objective to review the original recommendations and to determine the progress (or lack there of) that has occurred with regard to the protection of the infrastructures from HEMP.
2. Power companies in the United States should be provided with an incentive to increase their survivability to a HEMP attack over a period of years. As indicated by the EMP Commission, there are several activities that can be taken to achieve survivability. It is critical that power companies first assess their situation with regard to the threats, as not all power companies have the same vulnerabilities.
3. Any protection considered for HEMP (E1 and E3) should also include the consideration of EM weapon attacks producing IEMI and extreme geomagnetic storms. This is because there is a strong similarity between the protection methods required to achieve survivability for E1 HEMP and IEMI and also for E3 HEMP and extreme geomagnetic storms (discussed in the FERC reports).
4. It is important that advancements in power grid communications (known generally as Smart Grid) do not introduce new vulnerabilities in the power grid to HEMP and IEMI. NIST in Boulder, Colorado has a working group considering

these issues, and they should be requested to inform Congress of any emerging problems so that appropriate action can be taken.

5. A new emergency communications system is being developed in the United States known as First Net. The threats of HEMP and IEMI should be considered when developing this communications system, which will be needed if a terrorist attack occurs.
6. As actions are taken by various infrastructures, there should be a government agency that tracks the accomplishments and continuously informs Congress of the progress.
7. As the process moves forward, the need for new standards may become apparent. It is recommended that IEC SC 77C and the IEEE EMC Society be contacted, as they are well positioned to rapidly prepare any needed standards in this field of work.

References

Documents produced for FERC under contract to ORNL.

Savage, E. B., J. L. Gilbert, and W. A. Radasky, "The Early-Time (E1) Electromagnetic Pulse (HEMP) and its Impact on the U.S. Power Grid," Meta-R-320, Metatech Corporation, January 2010.

Gilbert, J. L., J. G. Kappenman, W. A. Radasky and E. B. Savage, "The Late-Time (E3) Electromagnetic Pulse (HEMP) and its Impact on the U.S. Power Grid," Metatech Corporation, Meta-R-321, January 2010.

Radasky, W. A. and E. B. Savage, "International Electromagnetic Interference (IEMI) and its Impact on the U.S. Power Grid," Metatech Corporation, Meta-R-323, January 2010.

Radasky, W. A. and E. B. Savage, "High-Frequency Protection Concepts for the Electric Power Grid," Metatech Corporation, Meta-R-324, January 2010.

Radasky, W. A. and J. G. Kappenman, "Protection Recommendations to Deal with Severe Electromagnetic Threats to the U.S. Power Grid," Metatech Corporation, Meta-R-325, January 2010.

Cigré Technical Brochure 600, "Protection of High Voltage Power Network Control Electronics Against Intentional Electromagnetic Interference (IEMI)," Working Group C4.206, November 2014.

IEEE Std 1642-2015, "IEEE Recommended Practice for Protecting Publicly Accessible Computer Systems from Intentional Electromagnetic Interference (IEMI)," 26 January 2015.

Radasky, W. A., "Fear of Frying: Electromagnetic Weapons Threaten Our Data Networks – Here's How to Stop Them," IEEE Spectrum Magazine, September 2014, pp. 46-51.

Radasky, W. A. and R. Hoad, "Status and Progress of IEC SC 77C High-Power Electromagnetics Publications in 2015," accepted for publication at the IEEE EMC International Conference in Dresden, Germany, August 2015.

CV for William A. Radasky

William A. Radasky received the B.S. degree with a double major in Electrical Engineering and Engineering Science from the U.S. Air Force Academy in 1968. He also received the M.S. and Ph.D. degrees in Electrical Engineering from the University of New Mexico in 1971 and the University of California, Santa Barbara in 1981, respectively with an emphasis on the theory and applications of electromagnetics.

He started his career in 1968 as an officer and research engineer at the Air Force Weapons Laboratory in Albuquerque, New Mexico and then worked for several private firms beginning in 1972. In 1984 he founded Metatech Corporation to perform research for government and commercial customers, and Metatech currently has offices in Goleta, California and Albuquerque, New Mexico. He is serving as President and Managing Engineer for the firm.

He has been active leading the standardization work in the IEC on high power transient phenomena since 1992, and he received the IEC Lord Kelvin Award in 2004 for his contributions. He is active in the IEEE EMC Society and Cigré SC C4, and has led several working groups in both organizations. As a research scientist he has published over 450 reports, papers and articles dealing with high power transients over his career. He has also been recognized as an IEEE Life Fellow for his research contributions. He is licensed as a Professional Engineer in the State of California.

Foundation for Resilient Societies
52 Technology Way
Nashua, NH 03060

May 12, 2015

Rep. Jason Chaffetz, Chairman
Rep. Elijah Cummings, Ranking Member
House Committee on Oversight & Government Reform
Rep. Cynthia Lummis, Chairman
Rep. Brenda Lawrence, Ranking Member
Subcommittee on the Interior
Rep. Ron DeSantis, Chairman
Rep. Stephen Lynch, Ranking Member
Subcommittee on National Security, and
Members of the House Committee on Oversight and Government Reform

Reference: May 13, 2015 Hearing on EMP Threat

The Foundation for Resilient Societies, a non-profit engaged in research and education on the resiliency of critical infrastructures, encloses an Electromagnetic Pulse and Geomagnetic Disturbance Protection Cost Model, Preliminary Version 0.16.

We also enclose a Fact Sheet that provides background information on the likelihood of EMP and GMD hazards, the consequences of these hazards, and the need for systematic assessment of what may need to be protected within the electric grid and supporting telecommunications and energy transport systems. The Fact Sheet provides click-through links to the Cost Model and summaries of the scope of protections at a lower cost program (about $10 billion dollars spread over five years) versus a higher cost program (about $30 billion dollars over the same time period).

We provide these materials for inclusion in the record of your May 13th hearing, "The EMP Threat: The State of Preparedness Against the Threat of an Electromagnetic Pulse Event."

Sincerely,

Thomas S. Popik, Chairman
Foundation for Resilient Societies
www.resilientsocieties.org

Enclosures

FACT SHEET

ON PRELIMINARY COSTING MODEL OF THE FOUNDATION FOR RESILIENT SOCIETIES TO PROTECT THE U.S. ELECTRIC GRID FROM MAN-MADE ELECTROMAGNETIC PULSE (EMP) HAZARDS AND SOLAR GEOMAGNETIC DISTURBANCES (GMD)

Foundation for Resilient Societies—May 12, 2015

The Foundation for Resilient Societies has developed an Electromagnetic Pulse (EMP) and Geomagnetic Disturbance (GMD) Protection Cost Model to assist public policymakers in prioritized protection of critical infrastructure in the United States. Infrastructure protection should start with the electric grid, the keystone infrastructure upon which all other infrastructures depend. While an "all hazards" grid protection approach must take into account physical security, cyber protection, solar geomagnetic storms, and man-made electromagnetic pulse hazards, our model starts by estimating the cost to mitigate risks from man-made electromagnetic pulse and solar geomagnetic storms.

Both man-made EMP and naturally-occurring GMD induce currents in long transmission lines and cause transformers at the end of these lines to overheat and prematurely fail. The "long pulses" from these two hazards, often known as E3 power surges, are generally mitigated using the same protective equipment. Man-made EMP also causes a "fast pulse," commonly known as E1, which impacts microelectronic components and systems. Unless equipment is installed to protect against E3 hazards, there is little benefit to solely protect against E1 because grid collapse would de-power all equipment. Much of electric grid equipment is already protected from a mid-range threat known as E2, by use of lighting arresters now widely deployed.

What is the probability of a solar geomagnetic storm that could cause the North American electric grid to separate with cascading collapse over one or more major grid interconnections? Multiple estimates for a super storm approximating the May 1921 Railroad Storm or the August-September 1859 Carrington Event place the probability at about 12 percent per decade. Therefore, without equipment redesign or protection, over the next fifty years the risk of cataclysmic grid outage is about 50 percent.

The projected costs of a regional or nationwide electric grid outage lasting months or years vary widely, but range from $1 trillion to over $10 trillion—plus potential widespread loss of life for the substantial majority of the 320 million people living in this nation. The costs of recovery without pre-disaster protection far exceed the costs of prevention, mitigation, and resiliency enhancements.

What is the probability of a man-made electromagnetic pulse attack, consisting of one or more EMP weapons detonated at high altitude? We do not know the answer. Both the governments

of North Korea and Iran, among others, have articulated interest in EMP weapons as vehicles of *asymmetric warfare.* Because the U.S. government has developed and deployed EMP protection systems for the Department of Defense and for other nationally critical facilities over many decades, one may hope that EMP threats or actual use of EMP weapons are deterred. We can expect that protecting even a fraction of our electrical grid and associated critical infrastructures will enhance deterrence.

Resilient Societies' Electromagnetic Pulse & Geomagnetic Disturbance Protection Cost Model does not address net expected benefits, because of uncertainties relative to combined probabilities of the events occurring and the investment required for anticipatory protection versus societal costs of protection failures. Nonetheless, given the extreme consequences, the benefits of protecting against man-made EMP and naturally-occurring GMD should be obvious to even the casual observer.

Our preliminary cost model, released on May 12, 2015 as Version 0.16 in Microsoft Excel format, provides a *range* of protective options, and hence a *range of projected costs*. Our projected costs, over the five year period 2016-2020 range from a low end of about $10 billion dollars to a high end of about $30 billion dollars. Some of the cost components are "best buys" under all conditions. For example, initiatives to protect the control systems, batteries, and communications for key grid "blackstart" facilities are less than one percent (1%) of total costs for both the low-end and high-end estimates.

Some protection costs are expensive for both scenarios—for example, the cost to protect large electric generation plants. Electric generation plants are complex and expensive machines, with multiple control systems and long cable runs exposed to E1. There are many different plant designs, even within general categories such as coal-fired, natural gas, petroleum, and hydroelectric. Modifications to control systems, such as implementing fiber optic communications, would need to be extensively tested for operational effectiveness and safety. When originally built, large electric generation plants cost hundreds of millions or billions of dollars and any retrofits would also be costly. As a result, we estimate that EMP protection of electric generation plants would cost in the millions of dollars per plant and we have reflected this in our cost model. Other specific assumptions and references are provided in the cost model itself.

No doubt some will disagree with details of our cost estimates. Nonetheless, we believe our methodology is robust. We take a systems approach, recognizing that to protect the electric grid, it is also necessary to protect supporting infrastructures such as telecommunications, natural gas pipelines, and rail transport. We estimate costs from the bottom up, listing the components to be protected and their approximate units, and then multiplying by per-unit

costs. We do not always assume 100% protection. Cost drivers are clearly delineated. For those who wish to run alternative scenarios, our model enables users to substitute assumptions about the protection components that are essential, or not, the percentages of equipment types to be protected, and variants in per-unit protection costs.

We note that our cost model projects higher costs of electric grid protection than did the Report of the Commission to Assess the Threat from Electromagnetic Pulse (EMP) Attack (April 2008). Converting the year 2007 dollars of the "EMP Commission Report" to year 2015 dollars, that Commission estimated grid protection costs ($2015) in a range from more than $2.7 billion dollars to more than $3.1 billion dollars.[1] Much additional information is now available on costs to mitigate solar storms and costs to harden control centers since the year 2008 EMP Commission Report. Moreover, our cost model includes significant cost elements that the EMP Commission only qualitatively addressed, including separate cost elements for telecommunications, natural gas pipelines and storage, and rail transport for resupply of fuel to coal-fired plants.[2]

A benchmark program of the U.S. Department of Energy for Smart Grid modernization provides a sense of comparability. Over a five year period in 2010-2015, the Smart Grid program provided up to 50% federal matching funds, with federal expenditures of $5.023 billion through March 31, 2015. When the program ends in coming months, the federal component will be about $5.2 billion with matching funds from electric utilities of around $7 billion dollars. This Smart Grid program could enable managed "load shedding" during emergencies and other benefits. But in terms of system reliability and system recovery, an EMP & GMD Protection Program could provide far more robust benefits at comparable program costs. A low-cost EMP & GMD Protection Program, if providing 50% federal grant eligibility, would cost taxpayers about as much as the Smart Grid Program while protecting the U.S. electric grid from both severe solar storms and man-made EMP attack.

For further information on the Foundation for Resilient Societies, Inc., see our website at: www.resilientsocieties.org.

For further information on the Resilient Societies EMP & GMD Protection Cost Model, please contact: Thomas S. Popik at: 1-855-OUTAGE-0. (1-855-688-2430).

---

[1] See Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures, April 2008, at pp. 60-61.

[2] Rail transport is vital for operation of most coal-fired plants. See Ibid., p 107: "Coal dominates all other categories of freight, accounting for 44 percent of Class I railroad tonnage in 2003. More than 90 percent of this coal, some 700 million tons, is delivered annually to coal-fired power plants. Power plants that depend on railroad-delivered coal account for more than one-third of our electricity production."

Cost Estimates from
"Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack; Critical National Infrastructures"
April 2008
Available at
http://www.empcommission.org/docs/A2473-EMP_Commission-7MB.pdf

	[redacted]				[redacted]			
Line Item—See references below.	**Total Units**	**Unit Cost to Protect**	**Protection Costs**	**Percent of Total Cost**	**Total Units**	**Unit Cost to Protect**	**Protection Costs**	**Percent of Total Cost**
1. Major Transformers and Other High Value Electric grid Components	"Several Thousand"	Unspecified	$250.000M	9%	"Several Thousand"	Unspecified	$500.000M	13%
2. Approximately 5,000 Generating Plants of Significance	5,000	$0.020M	$100.000M	3%	5,000	$0.050M	$250.000M	6%
3. Nonsynchronous Interfaces to Create Subregion Islands	6	$100.000M	$600.000M	21%	6	$150.000M	$900.000M	23%
4. Simulation and Training Centers for 3 Interconnections	3	Unspecified	$100.000M	3%	3	Unspecified	$250.000M	6%
5. Protection of Controls for Emergency Power Supplies	Unspecified	$0.030M	Unspecified		Unspecified	$0.030M	Unspecified	
6. Switchable Ground Resistors for High-Value Transformers	Unspecified	Unspecified	$75.000M	3%	5000	$150.000M	$250.000M	6%
7. Addition of New Black Start Generation	150	$12.000M	$1,800.000M	62%	150	$12.000M	$1,800.000M	46%
8. Addition of Emergency Generation	"Multitude of Sites"	$2.000M	n/a		"Multitude of Sites"	$5.000M	n/a	
9. Cost for Monitoring the State of the Electric Infrastructure	n/a	n/a	Unspecified		n/a	n/a	Unspecified	
10. Research and Development Activities	n/a	n/a	Unspecified		n/a	n/a	Unspecified	
Total Estimated Costs in 2007 Dollars			**$2,925.000M**	100%			**$3,950.000M**	100%
Cumulative Inflation from 2007 to 2015			14%				14%	
Total Estimated Costs in 2015 Dollars			**$3,334.500M**				**$4,503.000M**	

From pp. 60-61 of Critical National Infrastructures Report

It must be noted that the very wide variety of components; installation techniques; local system designs; age of components, subsystems, and controls located within buildings or exposed; and so forth all drastically affect the type and expense for implementing the recommended initiatives. Internal DHS and other governmental costs are assumed to be absorbed. A significant portion of the labor to affect the modifications is already in place. Often the modification will be part of a program for repair, replacement and modernization that is continuing regardless of the EMP mitigation program. The addition of nonsynchronous connection capability once defined is a contract function coupled with at-site staffing and control system interfaces. All of this effort factors into the cost estimates and results in fairly wide ranges in most instances. Only the costs for some of the larger or more system-specific initiatives are estimated here (in 2007 dollars).

1. There are several thousand major transformers and other high-value components on the transmission grid. Protective relays and sensors for these components are more than that number but less than twice. A continual program of replacement and upgrade with EMP-hardened components will substantially reduce the cost attributable uniquely to EMP. Labor for installation is already a part of the industry work force. The estimated cost for add-on and EMP-hardened replacement units and EMP protection schemes is in the range of $250 million to $500 million.

2. Approximately 5,000 generating plants of significance will need some form of added protection against EMP, particularly for their control systems. In some instances the fix is quite inexpensive and in others it will require major replacements. The estimated cost is in the range of $100 million to $250 million.

3. The addition of nonsynchronous interfaces to create subregion islands is not known with reasonable certainty, but it might be in the order of $100 million to $150 million per island. The pace of creating islands and their priority will be established by DHS in consultation with NERC and FERC. Moving to at least six or more fairly rapidly is a fair assumption. There will be annual operating costs of around $5 million per island.

4. The simulation and training centers are assumed at three — one for each interconnect — for a cost in the range of $100 million to $250 million plus annual operating costs of around $25 million per year.

5. Protection of controls for emergency power supplies should not be too expensive since hard-wired manual start and run capability should be in place for many, which is adequate. Furthermore, the test, adjust, and verification will be carried out by the entity that owns the emergency power supply as part of normal operating procedures. Retrofit of protective devices such as filters might be accomplished at a cost of less than $30,000 per generator for newer generators with vulnerable electronic controls. Hardening the connection to the rest of the facility power system requires a protected internal distribution system from the backup generator.

6. Switchable ground resistors for high-value transformers are estimated to cost in the range of $75 million to $150 million.

7. The addition of new black start generation with system integration and protected controls is estimated to cost around $12 million per installation. Probably no more than 150 such installations will need to be added throughout the United States and Canadian provinces.

8. The addition of emergency generation at the multitude of sites including fuel and transportation sites is probably around $2 million to $5 million each.

9. The cost for monitoring, on a continuous basis, the state of the electric infrastructure, its topology, and key elements plus for assessing the actual EMP vulnerability, validation of mitigation and protection, maintenance, and surveillance data for the system at large cannot be estimated since it falls under many existing government-funded activities, but in any event, it is not considered significant.

10. Research and development activities are a level-of-effort funding that needs to be decided by DHS. Redirection of existing funding is also likely to occur.

11. Funding for the initiatives above is to be divided between industry and government. Government is responsible for those activities that relate directly and uniquely to the purpose of assuring continuation of the necessary functioning of U.S. society in the face of an EMP attack or other broadly targeted physical or information systems attack. Industry is responsible for all other activities including reliability, efficiency and commercial interests. Industry is also the best source for advice on cost effective implementation of the initiatives.

Opening Statement
Ranking Member Brenda Lawrence (MI-1)
Subcommittee on the Interior
Joint hearing with
Subcommittee on National Security on
The EMP Threat: The State of Preparedness against the Threat of an Electromagnetic Pulse (EMP) Event
May 13, 2015

Madam Chairwoman, thank you for holding such an important hearing. I also want to thank our colleague, Representative Trent Franks, for his leadership in shining a light on an area of such critical concern.

Today, we discuss the potential threat of electro-magnetic pulse (E.M.P.) to our Nation's electric grid. The electric grid distributes electricity to every home, business and agency. It is a critical part of our infrastructure, supporting the economy and the health and welfare of our citizens.

According to scientists E.M.P.s are produced naturally by solar storms. However, there is greater concern over the E.M.P.s that can be generated by the explosion of a nuclear weapon high over the earth, or from devices aimed directly at our electrical power system.

E.M.P.s could severely damage the electric grid, and, in turn, a host of important systems. Our nation's defense system, for example, is almost entirely dependent on the national grid. An E.M.P. attack could cripple our defense capabilities and expose the U.S. to further threats.

Experts have estimated that a single E.M.P. strike in North America could interrupt power to as many as 130 million people in the U.S. alone and produce long term effects on our way of life. The supply

and distribution of food, water, communications, emergency services and government would be affected.

In 2001, Congress established the Commission to Assess the Threat to the United States from E.M.P Attack. According to the Commission's reports, there is much that can be done to protect the national electric grid and mitigate the damage caused by E.M.P.

We can upgrade our grid to withstand an E.M.P. attack. We need greater cooperation between government and industry in managing the adverse impacts of an E.M.P. event. And importantly, we must maintain a workforce with the technical competence to help us recover if an E.M.P. event does occur in the future.

I am looking forward to hearing from the witnesses and exploring all of the options that can produce the best outcomes in the event of an E.M.P. attack.

I yield back the balance of my time.

###

Testimony by Congressman Trent Franks
Committee on Oversight and Government Reform
National Security Subcommittee and Interior Subcommittee
The EMP Threat: The State of Preparedness
Against the Threat of an Electromagnetic Pulse Event
May 13, 2015

Good afternoon Chairmen DeSantis and Lummis, and Ranking Members Lynch and Lawrence, and the rest of my fellow Members on the committee. I believe the subject of this hearing is one of profound implication and importance so I want to sincerely thank you for allowing me to testify here today.

With each passing year, our society becomes increasingly dependent on technology - technology that would cannot function without the electric grid. Our household appliances, food distribution systems, telephone and computer networks, communication devices, water and sewage plants would grind to a halt without it. Nearly every single facet of modern human life is susceptible to being crippled by an Electromagnetic Pulse or Geomagnetic Disturbance event.

The effects of geomagnetic storms and electromagnetic pulses on electric infrastructure are well-documented, with nearly every space weather and EMP expert recognizing the dramatic disruptions these pulses can bring to electric grids. In 2008 the EMP Commission testified before The Armed Services Committee, of which I am a member, that the US society and economy are so critically dependent upon the availability of electricity that a significant collapse of the grid, precipitated by a major natural or man-made EMP event, could result in catastrophic civilian casualties. This conclusion is echoed by separate reports recently compiled by the DOD, DHS, DOE, National Academy of Sciences, along with many others. All came to very similar conclusions. We now have 11 government studies on the severe threat and vulnerabilities we face from EMP and GMD.

Recent Events
Mr. Chairman, as you can see, we have known about the potentially devastating effects of sufficiently intense electromagnetic pulse on electronic systems and its risk to our national security for some time. More troubling, our enemies know.

As we are all well aware, the Obama Administration is pursuing a deal with Iran that will legitimize them as a nuclear weapons threshold state. As the nuclear deal currently stands, it would leave Iran with approximately 6,000 running centrifuges – twice the number it needs for a full blown a nuclear weapons program capable of producing multiple warheads every year.

I am holding a recent Iranian Military Doctrine titled "Passive Defense" which has been translated by our very own National Intelligence University. This Iranian doctrine extols the former Soviet Union's deception programs that concealed from the U.S. the numbers and capabilities of Soviet nuclear weapons, enabling the USSR to cheat on treaties during the Cold War. The doctrine also mentions the use of nuclear weaponized electromagnetic pulse more than 20 times and states the importance of targeting critical infrastructure like the electric grid.

On April 16, 2013, North Korea flew a satellite on the optimum trajectory to evade U.S. radars and missile defenses, potentially practicing a surprise nuclear EMP attack on the United States. North Korea has now tested nuclear weapons on three known occasions.

The Threats
We as a nation have spent billions of dollars over the years hardening our nuclear triad, our missile-defense capabilities, and numerous other critical elements of our national security apparatus against the effects of electromagnetic pulse. However, our civilian grid, which the Defense Department relies upon for nearly 99% of its electricity needs, is completely vulnerable to the same kind of danger. This constitutes an invitation on the part of certain enemies of the United States to use the asymmetric capability of an EMP weapon against us.

We also face the threat of a natural EMP event. Since the last occurrence of a major geomagnetic storm in 1921, the nation's high voltage and extra high voltage systems have increased in size more than tenfold.

NASA in a July 2014 report warned that two years earlier, in 2012, the Earth narrowly missed a solar super-storm that could have generated a natural electromagnetic pulse (EMP) powerful enough to blackout electric grids and life sustaining critical infrastructures worldwide.

That same report estimated that the likelihood of a catastrophic solar super-storm hitting the Earth is 12 percent per decade. This virtually guarantees that the U.S. will encounter a potentially catastrophic natural EMP event within our lifetimes or that of our children.

Legislation
To this end, I have introduced The Critical Infrastructure Protection Act or CIPA and I would like to thank Chairman DeSantis for cosponsoring this bill. CIPA enhances the Department of Homeland Security's threat assessments for geomagnetic disturbances and electromagnetic pulse blackouts which will enable practical steps to protect the electric grid that serves our Nation. This legislation will also help the United States prepare for such an event by implementing large scale blackouts into existing national planning scenarios. Simply stated, it allows us to plan for protecting and recovering the electric grid and other critical infrastructure from an EMP event.

Close
Mr. Chairman, the challenge to ultimately and fully protect our people and nation from all of the various perils of natural or manmade electromagnetic pulse will be long and lingering. But the time to protect our nation from the worst case and most devastating scenario is now; the threat is real, and the implications are sobering.

Your actions today to protect America may gain you no fame or fanfare in the annals of history. However, it may happen in your lifetime that a natural or man-made EMP event so big has an effect so small that no one but a few will recognize the disaster that was averted. For the sake of our children and future generations, I pray it happens exactly that way.

Thank you and God bless all of you. Thank you and I yield back the balance of my time.

○