Testimony by Congressman Trent Franks
Homeland Security Committee Subcommittee on
Cybersecurity, Infrastructure Protection and Security Technologies
May 8, 2014

Good afternoon Chairman Perry, Ranking Member Clarke and fellow distinguished Members on the committee. I believe the subject of this hearing is one of profound implication and importance and consequently I am grateful to you all for allowing me to testify here today.

With each passing year, our society becomes increasingly dependent on technology and an abundant supply of electricity. Our entire American way of life relies upon electrical power and technology. 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 in America is susceptible to being crippled by a major Electromagnetic Pulse or Geomagnetic Disturbance event. We are so reliant on our electric power grid that we specifically consider it “critical infrastructure”.

Mr. Chairman and Members of the Committee, it strikes at my very core when I think of the men, women and children in cities and rural towns across America with a possibility of no access to food, water or transportation. In a matter of weeks or months at most, a worst case scenario could bring devastation beyond imagination.

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 and cataclysmic collapses 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, NAS, along with various other government agencies and independent researchers. 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 the potentially devastating effects of sufficiently intense electromagnetic pulse on the electronic systems and its risk to our national security. More troubling, our enemies know.

More than a year ago, an unknown number of shooters with AK-47s knocked out 17 large transformers during a highly-choreographed assault on the PG&E Metcalf Transmission Substation in California. While the power company was able to avoid blackouts, the damage to the facility took nearly four weeks to repair.

This is not an isolated incident and world-wide adversaries are taking notice in the vulnerability of our grid. Just last month, Connecticut officials released a report discussing their efforts to protect utility and distribution companies because hackers and cyber attackers around the world have made attempts to penetrate their systems.

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, particularly the type of electromagnetic pulse that might be generated against us by an enemy. 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. We are currently entering an interval of increased solar activity and are likely to encounter an increasing number of geomagnetic events on earth.

Legislation

To this end, I introduced The Critical Infrastructure Protection Act, HR 3410, which currently lays before your Committee. I'd like to thank Ranking Member Clarke, and my EMP Caucus co-chair for cosponsoring this critical legislation. HR 3410 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. It allows us to plan for protecting and recovering the electric grid and other critical infrastructure from an EMP event. In addition, it advances an educational awareness program to protect critical infrastructure and constructs a campaign to proactively educate emergency planners and emergency responders at all levels of government.

Summary

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 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.

"ELECTROMAGNETIC PULSE: THREAT TO CRITICAL INFRASTRUCTURE"
DR. PETER VINCENT PRY
TESTIMONY BEFORE THE
SUBCOMMITTEE ON CYBERSECURITY,
INFRASTRUCTURE PROTECTION AND SECURITY TECHNOLOGIES
HOUSE COMMITTEE ON HOMELAND SECURITY
May 8, 2014

Thank you for this opportunity to testify at your hearing on the threat posed by electromagnetic pulse (EMP) to critical infrastructure.

Natural EMP from a geomagnetic super-storm, like the1859 Carrington Event or 1921 Railroad Storm, and nuclear EMP attack from terrorists or rogue states, as practiced by North Korea during the nuclear crisis of 2013, are both existential threats that could kill 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.

Passage of the SHIELD Act to protect the national electric grid is urgently necessary. In 2010, after the House unanimously passed the GRID Act, if one Senator had not put a hold on the bill, today in 2014 the nation would already be protected, since it would take about 3.5 years to harden the grid.

Passage of the Critical Infrastructure Protection Act (CIPA) to create a new National Planning Scenario focused on EMP is urgently necessary. As the National Planning Scenarios are the basis for all federal, state and local emergency planning, training, and resource allocation, an EMP National Planning Scenario would immediately and significantly improve national preparedness for an EMP catastrophe.

The single most important thing Congress could do to protect the American people from EMP, and from all other threats to critical infrastructures, is pass the Critical Infrastructure Protection Act, which bill is or soon will be before this Committee for consideration.

Thousands of emergency planners and first responders at the federal, state, and local level want to protect our nation and their States and communities from the EMP threat. But they are seriously hindered and even prohibited from doing so because the EMP threat is not among the 15 canonical National Planning Scenarios utilized by the Department of Homeland Security.

Passage of the Critical Infrastructure Protection Act would immediately mobilize thousands of emergency planners and first responders at all levels of government, and educate millions of others, about the EMP threat and how to prepare for it.

Passage of the Critical Infrastructure Protection Act would immediately help States that are frustrated with lack of action on EMP in Washington, and are trying to launch initiatives protecting their electrical grids from EMP, as is being attempted now in Maine, Virginia, Oklahoma, and Florida.

Passage of the Critical Infrastructure Protection Act would educate all States about the EMP threat and help them protect their critical infrastructures.

For example, projects in New York and Massachusetts to harden their State grids against severe weather caused by climate change should include protection against an EMP event, which is the worst threat to the grid. If the grid is protected against EMP, it will mitigate all lesser threats, including cyber attack, sabotage, and severe weather.

Given the amounts of money being spent in New York and Massachusetts on grid hardening against severe weather, significant EMP protection can probably be accomplished now within their current budgets. But the cost of EMP protection will increase significantly if they delay and attempt remediation later.

EMP is a clear and present danger. A Carrington-class coronal mass ejection narrowly missed the Earth in July 2012. Last April, during the nuclear crisis with North Korea over Kim Jong-Un's threatened nuclear strikes against the United States, Pyongyang apparently practiced an EMP attack with its KSM-3 satellite, that passed over the U.S. heartland and over the Washington, D.C.-New York City corridor. Iran, estimated to be within two months of nuclear weapons by the Administration, has a demonstrated capability to launch an EMP attack from a vessel at sea. The Iranian Revolutionary Guard Navy commenced patrols off the East Coast of the United States in February.

Thank you for your attention to EMP, which is the least understood but gravest threat to our society. This concludes my remarks.

WHAT IS EMP?

Nuclear, Natural, and Non-Nuclear EMP

An electromagnetic pulse (EMP) is a super-energetic radio wave that can destroy, damage or cause the malfunction of electronic systems by overloading their circuits. EMP is harmless to people biologically, passing through their bodies without injury, like a radio wave. But by damaging electronic systems that make modern society possible, that enable computers to function and airliners to fly for example, EMP can cause mass destruction of property and life.

A single nuclear weapon detonated at high-altitude will generate an electromagnetic pulse that can cause catastrophic damage across the entire contiguous United States to the critical infrastructures--electric power, telecommunications, transportation, banking and finance, food and water--that sustain modern civilization and the lives of 310 million Americans. Nature can also generate an EMP causing similarly catastrophic consequences across the entire contiguous United States--or even across the entire planet--by means of a solar flare from the Sun that causes on Earth a great geomagnetic storm. Non-nuclear weapons, often referred to as radiofrequency weapons, can also generate an EMP, much more limited in range than a nuclear weapon, that can damage electronics, and could cause the collapse of critical infrastructures locally, perhaps with cascading effects over an area as large as a major city.

Nuclear EMP

Any nuclear warhead detonated at high-altitude, 30 kilometers or more above the Earth's surface, will generate an electromagnetic pulse. The immediate effects of EMP are disruption of, and damage to, electronic systems and electrical infrastructure. EMP is not reported in the scientific literature to have direct harmful effects on people. Because an EMP attack would detonate a nuclear warhead at high-altitude, no other nuclear effects--such as blast, thermal radiation, or radioactive fallout--would be experienced by people on the ground or flying through the atmosphere. However, because modern civilization and life itself now depends upon electricity and electronics, an EMP attack is a high-tech means of killing millions of people the old fashioned way--through starvation, disease, and societal collapse.

Gamma rays, and the fireball from a high-altitude nuclear detonation, interact with the atmosphere to produce a super-energetic radio wave--the EMP--that covers everything within line-of-sight from the explosion to the Earth's horizon. Thus, even a relatively low-altitude EMP attack, where the nuclear warhead is detonated at an altitude of 30 kilometers, will generate a damaging EMP field over a vast area, covering a region equivalent to New England, all of New York, and half of Pennsylvania. A nuclear weapon detonated at an altitude of 400 kilometers over the center of the United States would place an EMP field over the entire contiguous United States and parts of Canada and Mexico.

The EMP generated by a nuclear weapon has three components, designated by the U.S. scientific-technical community E1, E2, and E3.

E1 is caused by gamma rays, emitted by the nuclear warhead, that knocks electrons off of molecules in the upper atmosphere, causing the electrons to rotate rapidly around the lines of the Earth's magnetic field, a phenomenon termed the Compton Effect. The E1 component of nuclear EMP is a shockwave, transmitting thousands of volts of energy in mere nanoseconds of time, and having a high-frequency (short) wavelength that can couple directly into small objects, like personal computers, automobiles, and transformers. E1 is unique to nuclear weapons and is too fast and too energetic to be arrested by protective devices used for lightening.

The E2 component of a nuclear EMP is comparable to lightening in its energetic content and medium (milliseconds) frequency and wavelength. Protective devices used for lightening are effective against E2.

E3 is caused by the fireball of a nuclear explosion, the expanding and then collapsing fireball causing the Earth's magnetic field to oscillate, generating electric currents in the very large objects that can couple into the low frequency, long (seconds) wavelength part of the EMP that is E3. The E3 waveform can couple directly only into objects having at least one dimension of great length. Electric power and telecommunications lines, that run for kilometers in many directions, are ideally suited for receiving E3. Although E3 compared to E1 appears to deliver little energy, just volts per meter, this is multiplied manifold by power and telecommunications lines that are typically many kilometers long, building up E3 currents that can melt Extremely High Voltage (EHV) transformers, typically designed to handle 750,000 volts. Small electronics can also be destroyed by E3 if they are connected in any way to an E3 receiver--like a personal computer plugged into an electric outlet, which of course is connected to power lines that are ideal E3 receivers, or like the electronic servo-mechanisms that operate the controls of large passenger airliners, that can receive E3 through the metal skin of the aircraft wings and body.

Protective devices used for lightening are not effective against E3, that can build up energy sufficient to overwhelm lightening arrestors and bypass them through electrical arcing.

EMP and its effects were observed during the U.S. and Soviet atmospheric test programs in 1962. The 1962 U.S. STARFISH nuclear detonation--not designed or intended as an EMP generator--at an altitude of about 400 kilometers above Johnston Island in the Pacific Ocean, surprised the U.S. scientific community by producing EMP. Some electronic systems in the Hawaiian Islands, 1400 kilometers distant, were affected, causing the failure of street lights, tripping circuit breakers, triggering burglar alarms, and damage to telecommunications. In their testing that year, the Soviets executed a series of nuclear detonations in which they exploded 300 kiloton weapons at approximately 300, 150, and 60 kilometers above their test site in South Central Asia. They report that on each shot they observed damage to overhead and underground buried cables at distances of 600 kilometers. They also observed surge arrestor burnout, spark-gap breakdown, blown fuses, and power supply breakdowns.

In the years since 1962, the U.S. scientific and defense community established incontrovertibly, by means of nuclear tests and EMP simulators, that an EMP attack could have catastrophic effects by destroying electronic systems over broad regions--potentially over the entire contiguous United States.

Because so much information about EMP was largely classified for so long, myths abound about EMP, that the EMP Commission has endeavored to correct in its unclassified reports and briefings. For example, a high-yield nuclear weapon is not necessary to make an EMP attack. Although a high-yield weapon will generally make a more powerful EMP field than a low-yield nuclear weapon, ALL nuclear weapons produce gamma rays and EMP. The EMP Commission found, by testing modern electronics in simulators, that ANY nuclear weapon can potentially make a catastrophic EMP attack on the United States. Even a very low yield nuclear weapon--like a 1-kiloton nuclear artillery shell--will produce enough EMP to pose a catastrophic threat. This is so in part because the U.S. electric grid is so aged and overburdened, and because the high-tech electronics that support the electric grid and other critical infrastructures are over one million times more vulnerable to EMP than the electronics of the 1960s.

The EMP Commission also found that, contrary to the claim that high-yield nuclear weapons are necessary for an EMP attack, that very low-yield nuclear weapons of special design can produce significantly more EMP than high-yield nuclear weapons. The EMP Commission found further that Russia, probably China, and possibly North Korea are already in possession of such weapons. Russian military writings call these "Super-EMP" nuclear weapons, and credibly claim that they can generate 200 kilovolts per meter--many times the 30 KVs/meter attributed to a high-yield (20 megaton) nuclear weapon of normal design. Yet a Super-EMP warhead can have a tiny explosive yield, perhaps only 1 kiloton, because it is specially designed to produce primarily gamma rays that generate the E1 electromagnetic shockwave component of the EMP effect. Super-EMP weapons are specialized to generate an overwhelming E1, and produce no E2 or E3 but do not need to, as their E1 is so potent.

In 2004, credible Russian sources warned the EMP Commission that design information and "brain drain" from Russia had transferred to North Korea the capability to

build a Super-EMP nuclear weapon "within a few years." In 2006 and again in 2008, North Korea tested a nuclear device of very low yield, 1-3 kilotons, and declared these tests successful. South Korean military intelligence, in open source reporting, independently corroborates the Russian warning that North Korea is developing a Super-EMP nuclear warhead. North Korea's proclivity to sell anything to anyone, including missiles and nuclear technology to fellow rogue nations Iran and Syria, makes Pyongyang's possession of Super-EMP nuclear weapons especially worrisome.

Another myth is that rogue states or terrorists need a sophisticated intercontinental ballistic missile to make an EMP attack. In fact, any missile, including short-range missiles that can deliver a nuclear warhead to an altitude of 30 kilometers or more, can make a catastrophic EMP attack on the United States, by launching off a ship or freighter. Indeed, Iran has practiced ship-launched EMP attacks using Scud missiles--which are in the possession of scores of nations and even terrorist groups. An EMP attack launched off a ship, since Scuds are commonplace and a warhead detonated in outer space would leave no bomb debris for forensic analysis, could enable rogue states or terrorists to destroy U.S. critical infrastructures and kill millions of Americans anonymously.

Natural EMP

Mother Nature can also pose an EMP threat. The Sun emits solar flares and coronal mass ejections that can strike the Earth's magnetosphere and generate a natural EMP in the form of a geomagnetic storm. Geomagnetic storms rarely effect the United States, but regularly damage nations located at high northern latitudes, such as Canada, Norway, Sweden, Finland and Russia. Damage from a normal geomagnetic storm can be severe. For example, in 1989 a geomagnetic storm over Canada destroyed the electric power grid in Quebec.

The EMP Commission was the first to discover and report in 2004 that every hundred years or so the Sun produces a *great* geomagnetic storm. Great geomagnetic storms produce effects similar to the E3 EMP from a multi-megaton nuclear weapon, and so large that it would cover the entire United States--possibly even the entire planet. Geomagnetic storms, even great geomagnetic storms, generate no E1 or E2, only E3, technically called the magnetohydrodynamic EMP.

Nonetheless, E3 alone from a great geomagnetic storm is sufficient to end modern civilization. The EMP produced, given the current state of unpreparedness by the U.S. and every nation on Earth, could collapse power grids everywhere on the planet and destroy EHV transformers and other electronic systems that would require years to repair or replace.

Modern civilization cannot exist for a protracted period without electricity. Within days of a blackout across the U.S., a blackout that could encompass the entire planet, emergency generators would run out of fuel, telecommunications would cease as would transportation due to gridlock, and eventually no fuel. Cities would have no running water and soon, within a few days, exhaust their food supplies. Police, Fire, Emergency Services and hospitals cannot long operate in a blackout. Government and Industry also need electricity in order to operate.

The EMP Commission warns that a natural or nuclear EMP event, given current unpreparedness, would likely result in societal collapse.

The last great geomagnetic storm was in 1859, called the "Carrington Event" after the astronomer who noted the phenomenon. The 1859 great geomagnetic storm caused fires in telegraph stations and burned the just laid transatlantic cable, but its effects were not catastrophic because electronic systems were few and not essential to society in 1859. Great geomagnetic storms are recognizable in historical records because they produce highly unusual effects, like the appearance of the Aurora Borealis at the equator, that even common people often record in letters and diaries.

No great geomagnetic storm has occurred in the modern era, in which society depends for its very existence on electronics. Most specialists believe a great geomagnetic storm is overdue, since this once a century phenomenon last occurred in 1859. Many scientists believe a great geomagnetic storm is most likely to occur during the solar maximum, when solar flares and coronal mass ejections that cause geomagnetic storms increase sharply in frequency. The solar maximum recurs every 11 years, next in 2012-2013.

NASA and the National Academy of Sciences (NAS) published a blue-ribbon study independently confirming the warning of the EMP Commission about the threat posed by a great geomagnetic storm. The EMP Commission and the NASA-NAS reports, and several subsequent independent studies, conclude that if a great geomagnetic storm like the 1859 Carrington Event happened today, millions could die.

Non-Nuclear EMP Weapons

Radiofrequency weapons of widely varying designs--some using conventional explosions to generate an EMP, others using microwave emitters to direct energy at a target, for example--can destroy, damage and disrupt electronic systems at short ranges. Non-nuclear EMP weapons seldom have ranges or a radius of effect greater than one kilometer, and usually much less than this.

Some scientists credibly claim that non-nuclear EMP weapons can be developed having a radius of effect of tens of kilometers. However, no nation has yet demonstrated such a capability, including the United States, which has worked to develop advanced radiofrequency weapons for many years. Even such advanced non-nuclear EMP weapons would still be limited and localized in their effects, compared to the nationwide effects of a nuclear EMP attack or the planetary effects of a great geomagnetic storm.

Microwave radiation is the lethal mechanism usually employed by non-nuclear EMP weapons, an effect somewhat comparable but not identical to E1 from a nuclear weapon. Radiofrequency weapons produce no E2 or E3 pulse.

Terrorists, criminals, and even lone individuals can build a non-nuclear EMP weapon without great trouble or expense, working from unclassified designs publicly available on the internet, and using parts available at any electronics store. In 2000, the Terrorism Panel of the House Armed Services Committee sponsored an experiment, recruiting a small team of amateur electronics enthusiasts to attempt constructing a radiofrequency weapon, relying only on unclassified design information and parts purchased from Radio Shack. The team, in one year, built two radiofrequency weapons of radically different designs. One was designed to fit inside the shipping crate for a Xerox machine, so it could be delivered to the Pentagon mail room where (in those more unguarded days before 9/11) it could slowly fry the Pentagon's computers. The other

radiofrequency weapon was designed to fit inside a small Volkswagon bus, so it could be driven down Wall Street and disrupt computers--and perhaps the national economy.

Both designs were demonstrated and tested successfully during a special congressional hearing for this purpose at the U.S. Army's Aberdeen Proving Ground.

Radiofrequency weapons are not merely a hypothetical threat. Terrorists, criminals, and disgruntled individuals have used home-made radiofrequency weapons. The U.S. military and foreign militaries have a wide variety of such weaponry.

Moreover, non-nuclear EMP devices that could be used as radiofrequency weapons are publicly marketed for sale to anyone, usually advertised as "EMP simulators." For example, one such simulator is advertised for public sale as an "EMP Suitcase." This EMP simulator is designed to look like a suitcase, can be carried and operated by one person, and is purpose built with a high energy radiofrequency output to destroy electronics. However, it has only a short radius of effect. Nonetheless, a terrorist or deranged individual who knows what he is doing, who has studied the electric grid for a major metropolitan area, could-- armed with the "EMP Suitcase"--blackout a major city.

A Clear and Present Danger

Emphasis is warranted that the nuclear EMP threat is not merely theoretical--it is real, a clear and present danger. Nuclear EMP attack is the perfect asymmetric weapon for state actors who wish to level the battlefield by neutralizing the great technological advantage enjoyed by U.S. military forces. EMP is also the ideal means, the only means, whereby rogue states or terrorists could use a single nuclear weapon to destroy the United States and prevail in the War on Terrorism or some other conflict with a single blow. The EMP Commission also warned that states or terrorists could exploit U.S. vulnerability to EMP attack for coercion or blackmail: "Therefore, terrorists or state actors that possess relatively unsophisticated missiles armed with nuclear weapons may well calculate that, instead of destroying a city or military base, they may obtain the greatest political-military utility from one or a few such weapons by using them--or threatening their use--in an EMP attack."

The EMP Commission found that states such as Russia, China, North Korea, and Iran have incorporated EMP attack into their military doctrines, and openly describe making EMP attacks against the United States. Indeed, the EMP Commission was established by Congress partly in response to a Russian nuclear EMP threat made to an official Congressional Delegation on May 2, 1999, in the midst of the Balkans crisis. Vladimir Lukin, head of the Russian delegation and a former Ambassador to the United States, warned: "Hypothetically, if Russia really wanted to hurt the United States in retaliation for NATO's bombing of Yugoslavia, Russia could fire an SLBM and detonate a single nuclear warhead at high altitude over the United States. The resulting EMP would massively disrupt U.S. communications and computer systems, shutting down everything."

China's military doctrine also openly describes EMP attack as the ultimate asymmetric weapon, as it strikes at the very technology that is the basis of U.S. power. Where EMP is concerned, "The United States is more vulnerable to attacks than any other country in the world":

> *Some people might think that things similar to the "Pearl Harbor Incident' are unlikely to take place during the information age. Yet it could be*

regarded as the 'Pearl Harbor Incident' of the 21st Century if a surprise attack is conducted against the enemy's crucial information systems of command, control, and communications by such means as...electromagnetic pulse weapons...Even a superpower like the United States, which possesses nuclear missiles and powerful armed forces, cannot guarantee its immunity ...In their own words, a highly computerized open society like the United States is extremely vulnerable to electronic attacks from all sides. This is because the U.S. economy, from banks to telephone systems and from power plants to iron and steel works, relies entirely on computer networks.... When a country grows increasingly powerful economically and technologically...it will become increasingly dependent on modern information systems....The United States is more vulnerable to attacks than any other country in the world.

Iran--the world's leading sponsor of international terrorism--in military writings openly describes EMP as a terrorist weapon, and as the ultimate weapon for prevailing over the West: "If the world's industrial countries fail to devise effective ways to defend themselves against dangerous electronic assaults, then they will disintegrate within a few years....American soldiers would not be able to find food to eat nor would they be able to fire a single shot."

The threats are not merely words. The EMP Commission assesses that Russia has, as it openly declares in military writings, probably developed what Russia describes as a "Super-EMP" nuclear weapon--specifically designed to generate extraordinarily high EMP fields in order to paralyze even the best protected U.S. strategic and military forces. China probably also has Super-EMP weapons. North Korea too may possess or be developing a Super-EMP nuclear weapon, as alleged by credible Russian sources to the EMP Commission, and by open source reporting from South Korean military intelligence. But any nuclear weapon, even a low-yield first generation device, could suffice to make a catastrophic EMP attack on the United States. Iran, although it is assessed as not yet having the bomb, is actively testing missile delivery systems and has practiced launches of its best missile, the Shahab-III, fuzing for high-altitude detonations, in exercises that look suspiciously like training for making EMP attacks. As noted earlier, Iran has also practiced launching from a ship a Scud, the world's most common missile--possessed by over 60 nations, terrorist groups, and private collectors. A Scud might be the ideal choice for a ship-launched EMP attack against the U.S. intended to be executed anonymously, to escape any last gasp U.S. retaliation. Unlike a nuclear weapon detonated in a city, a high-altitude EMP attack leaves no bomb debris for forensic analysis, no perpetrator "fingerprints."

EMP Vulnerabilities

Today's microelectronics are the foundation of our modern civilization, but are over one million times more vulnerable to EMP than the far more primitive and robust electronics of the 1960s, that proved vulnerable during nuclear EMP tests of that era. Tests conducted by the EMP Commission confirmed empirically the theory that, as modern microelectronics become ever smaller and more efficient, and operate ever faster on lower voltages, they also become ever more vulnerable, and can be destroyed or disrupted by much lower EMP field strengths.

Microelectronics and electronic systems are everywhere, and run virtually everything in the modern world. All of the civilian critical infrastructures that sustain the

economy of the United States, and the lives of 310 million Americans, depend, directly or indirectly, upon electricity and electronic systems.

Of special concern is the vulnerability to EMP of the Extra High-Voltage (EHV) transformers, that are indispensable to the operation of the electric grid. EHV transformers drive electric current over long distances, from the point of generation to consumers (from the Niagara Falls hydroelectric facility to New York City, for example). The electric grid cannot operate without EHV transformers--which could be destroyed by an EMP event. The United States no longer manufactures EHV transformers. They must be manufactured and imported from overseas, from Germany or South Korea, the only two nations in the world that manufacture such transformers for export. Each EHV transformer must be custom made for its unique role in the grid. A single EHV transformer typically requires 18 months to manufacture. The loss of large numbers of EHV transformers to an EMP event would plunge the United States into a protracted blackout lasting years, with perhaps no hope of eventual recovery, as the society and population probably could not survive for even one year without electricity.

Another key vulnerability to EMP are Supervisory Control And Data Acquisition systems (SCADAs). SCADAs essentially are small computers, numbering in the millions and ubiquitous everywhere in the critical infrastructures, that perform jobs previously performed by hundreds of thousands of human technicians during the 1960s and before, in the era prior to the microelectronics revolution. SCADAs do things like regulating the flow of electricity into a transformer, controlling the flow of gas through a pipeline, or running traffic control lights. SCADAs enable a few dozen people to run the critical infrastructures for an entire city, whereas previously hundreds or even thousands of technicians were necessary. Unfortunately, SCADAs are especially vulnerable to EMP.

EHV transformers and SCADAs are the most important vulnerabilities to EMP, but are by no means the only vulnerabilities. Each of the critical infrastructures has their own unique vulnerabilities to EMP:

The national electric grid, with its transformers and generators and electronic controls and thousands of miles of power lines, is a vast electronic machine--more vulnerable to EMP than any other critical infrastructure. Yet the electric grid is the most important of all critical infrastructures, and is in fact the keystone supporting modern civilization, as it powers all the other critical infrastructures. As of now it is our technological Achilles Heel. The EMP Commission found that, if the electric grid collapses, so too will collapse all the other critical infrastructures. But, if the electric grid can be protected and recovered, so too all the other critical infrastructures can also be restored.

Transportation is a critical infrastructure because modern civilization cannot exist without the goods and services moved by road, rail, ship and air. Cars, trucks, locomotives, ships and aircraft all have electronic components, motors, and controls that are potentially vulnerable to EMP. Traffic control systems that avert traffic jams and collisions for road, rail and air depend upon electronic systems, that the EMP Commission discovered are especially vulnerable to EMP. Gas stations, fuel pipelines, and refineries that make petroleum products depend upon electronic components and cannot operate without electricity. Given our current state of unpreparedness, in the aftermath of a natural or nuclear EMP event, transportation systems would be paralyzed.

Communications is a critical infrastructure because modern economies and the cohesion and operation of modern societies depend to a degree unprecedented in history on the rapid movement of information--accomplished today mostly by electronic means. Telephones, cell phones, personal computers, television and radio are all directly vulnerable to EMP, and cannot operate without electricity. Satellites that operate at Low-Earth-Orbit (LEO) for communications, weather, scientific and military purposes are vulnerable to EMP and to collateral effects from an EMP attack. Within weeks of an EMP event, the LEO satellites, which comprise most satellites, would probably be inoperable. In the aftermath of a nuclear or natural EMP event, under present levels of preparedness, communications would be severely limited, restricted mainly to those few military communications networks that are hardened against EMP.

Banking and finance are the critical infrastructure that sustain modern economies. Whether it is the stock market, the financial records of a multinational corporation, or the ATM card of an individual--financial transactions and record keeping all depend now at the macro- and micro-level upon computers and electronic automated systems. Many of these are directly vulnerable to EMP, and none can operate without electricity. The EMP Commission found that an EMP event could transform the modern electronic economy into a feudal economy based on barter.

Food has always been vital to every person and every civilization. The critical infrastructure for producing, delivering, and storing food depends upon a complex web of technology, including machines for planting and harvesting and packaging, refrigerated vehicles for long haul transportation, and temperature controlled warehouses. Modern technology enables over 98 percent of the U.S. national population to be fed by less than 2 percent of the population. Huge regional warehouses that resupply supermarkets constitute the national food reserves, enough food to feed the nation for 30-60 days at normal consumption rates, the warehoused food preserved by refrigeration and temperature control systems that typically have enough emergency electrical power (diesel or gas generators) to last only about an average of three days. Experience with storm-induced blackouts proves that when these big regional food warehouses lose electrical power, most of the food supply will rapidly spoil. Farmers, less than 2 percent of the population as noted above, cannot feed 310 million Americans if deprived of the means that currently makes possible this technological miracle.

Water too has always been a basic necessity to every person and civilization, even more crucial than food. The critical infrastructure for purifying and delivering potable water, and for disposing of and treating waste water, is a vast networked machine powered by electricity that uses electrical pumps, screens, filters, paddles, and sprayers to purify and deliver drinkable water, and to remove and treat waste water. Much of the machinery in the water infrastructure is directly vulnerable to EMP. The system cannot operate without vast amounts of electricity supplied by the power grid. A natural or nuclear EMP event would immediately deprive most of the U.S. national population of running water. Many natural sources of water--lakes, streams and rivers--would be dangerously polluted by toxic wastes from sewage, industry, and hospitals that would backflow from or bypass wastewater treatment plants, that could no longer intake and treat pollutants without electric power. Many natural water sources that would normally be safe to drink, after an EMP event, would be polluted with human wastes including feces, industrial wastes including arsenic and heavy metals, and hospital wastes including pathogens.

Emergency services such as police, fire, and hospitals are the critical infrastructure that upholds the most basic functions of government and society--preserving law and order, protecting property and life. Experience from protracted storm-induced blackouts has shown, for example in the aftermath of Hurricanes Andrew and Katrina, that when the lights go out and communications systems fail and there is no gas for squad cars, fire trucks, and ambulances, the worst elements of society and the worst human instincts rapidly takeover. The EMP Commission found that, given our current state of unpreparedness, a natural or nuclear EMP event could create anarchic conditions that would profoundly challenge the existence of social order.

TESTIMONY OF DR. MICHAEL J. FRANKEL

HOUSE HOMELAND SECURITY COMMITTEE HEARING

SUB-COMMITTEE ON CYBER SECURITY, INFRASTRUCTURE PROTECTION,

AND SECURITY TECHNOLOGIES, HOUSE CANNON OFFICE BUILDING,

ROOM 311, MAY 8, 2014

Mr. Chairman and Honorable Members of the Committee, thank you for the opportunity to testify today about an important but relatively neglected vulnerability that affects the resilience of all of our nation's critical infrastructures. My name is Mike Frankel. I'm a theoretical physicist by trade and presently a member of the senior scientific staff at Penn State University's Applied Research Laboratory. I've spent a career in government service developing technical and scientific expertise on the effects of nuclear weapons, managing WMD programs, and performing scientific research in a variety of national security positions with the Navy, the old Defense Nuclear Agency, and the Office of the Secretary of Defense. I appear before you today pursuant my service as the Executive Director of the EMP Commission during its entire span of activity, commencing with authorization if the Floyd D. Spence National Defense Authorization Act of 2001 and culminating with delivery of its final, classified, assessment to the Congress in 2009 The conclusions of the Commission were documented in a series of five volumes, three of them classified, and in particular the Commission's perspectives related to infrastructure protection were documented in an unclassified volume *"Critical National Infrastructures",* released in November of 2008. What I'd like to do is expand on some of the Commission's conclusions in light of recent developments since submitting our final report. I should also like to emphasize a new topic that was not referenced in that final report, and that is the nexus between the cyber security threat and EMP.

One of the major insights of the EMP Commission was to highlight the unique danger to the electric grid caused by simultaneous failures induced by the large number of components that fall within an EMP's damaging footprint on the ground. As first reported in the journal Foreign Affairs and picked up a month later by the Wall Street Journal, on the night of April 16, 2013, a locked PG&E substation was infiltrated and a number of high voltage transformers attacked by still unidentified individuals firing rifles. Damaged transformers went off line but the SCADA controls automatically re-routed the electrical distribution along alternate paths. In this case, standard engineering practice

which designs around the possibility of single point failure, kicked in just as it should. and little effect was noticed by the general population. However, it took nearly a full month to repair the damaged transformers and return them to service. An important analytic contribution of the Commission was to highlight the possibility of highly multiple numbers of component failures, as might be expected within the wide area encompassed by an EMP event footprint. No one designed against such a possibility and it was the Commission's conclusion, based on its own analyses and on a close collaboration with power industry engineers, that such a scenario would inevitably lead to very wide spread, and very long term collapse of the nation's electric grid, with potentially devastating economic and ultimately physical and health consequences. The PG&E incident should remind us that the Commission's analytic insight extends far beyond EMP. While in this case only a single substation was attacked, had there been a coordinated physical attack against many simultaneous targets, or for that matter by localized EMP sources such as readily available HPM/RF sources, it seems inevitable that electric service to much larger fraction of the population would have been compromised and for an indefinitely prolonged period. And of course, the same result could be achieved by simultaneous cyber-attack, with much reduced physical exposure by the perpetrators. So there's a real vulnerability there that needs to be addressed.

I should also like to turn some attention to the generally unremarked overlap between electromagnetic vulnerability of the type described by the EMP Commission and the more general issue of cyber vulnerability. While not often considered in tandem, it is more correct to consider EMP vulnerabilities as one end of a continuous spectrum of cyber threats to our electronic based infrastructures. They share both an overlap in the effects produced – the failure of electronic systems to perform their function and possibly incurring actual physical damage – as well as their mode of inflicting damage. They both reach out through the connecting electronic distribution systems, and impress unwanted voltages and currents on the connecting wires. In the usual cyber case, those unwanted currents contain information – usually in the form of malicious code – that instructs the system to perform actions unwanted and unanticipated by its owner. In the EMP case, the impressed signal does not contain coded information. It is merely a dump of random noise which may flip bit states, or damage components, and also ensures the system will not behave in the way the owner expects. This electronic noise dump may thus be thought of as a "stupid cyber". When addressing the vulnerability of our infrastructures to the cyber threat, it is important that we not neglect the EMP end of the cyber threat spectrum. And there is another important overlap with the cyber threat. With the grid on the cusp of technological change in the evolution to the "smart grid", the proliferation of sensors and controls which will manage the new grid architecture must be protected against cyber at the same time they must be protected against EMP. Cyber and EMP threats have the unique capability to precipitate highly multiple failures of these many new control systems over a widely distributed

geographical area, and such simultaneous failures, as previously discussed, are likely to signal a wider and more long lasting catastrophe.

Another important legacy of the EMP Commission was to first highlight the danger to our electric grid due to solar storms, which may impress large - and effectively DC - currents on the long runs of conducting cable that make up the distribution system. While this phenomenon has long been known, and protected against, by engineering practices in the power industry, the extreme 100-year storm first analyzed by the Commission is now widely recognized to represent a major danger to our national electrical system for which adequate protective measures have not been taken and whose consequences – the likely collapse of much of the national grid, possibly for a greatly extended period, may rightly be termed catastrophic. At this point, the only scientific controversy attending the likelihood of our system being subject to a so-called super solar storm, is related to the time-constant. But these events have already occurred within the last century or so, they will occur again. We should be ready.

The most important legacy of the EMP Commission however, was in the recommendations which were provided that would, if acted upon, protect key assets of both the civilian and military infrastructures, And it is here that I should like to point to an important divergence in the government's response. The (classified) recommendations that were provided to the Department of Defense were formally considered, in the large main concurred with, and then acted upon. The Secretary of Defense issued a classified action plan, out-year funding was POM'd in the FYDP, an office and an official of responsibility were appointed, a standing Defense Science Board committee was stood up, an active research program is maintained, and survivability and certification instructions were issued by both DOD and by USSTRATCOM. Today, while vigilant oversight continues to be warranted, an EMP awareness pervades our acquisition system and operational doctrine. The response on the civilian side of the equation was not so rosy. The final report of EMP Commission contained seventy five recommendations to improve the survivability, operability, resilience, and recovery of all the critical infrastructures, and in particular of the most key of all, the electrical grid. Most of these recommendations were pointed towards the Department of Homeland Security. While there have been some conversations, it has been hard to detect much of an active resonance at all issuing from the Department. They have not, as far as I know, even designated EMP as a one of their ten of fifteen disaster scenarios for advanced planning circumstances. And this at a time when they do include a low altitude nuclear disaster -certainly disastrous but not one that would produce wide ranging EMP.

In the end, it is hard to deal with seventy five recommendations, all at once. But the solution is not to ignore all of them. If there is only a single essentially a no-cost step I would leave this Committee with, it would be to task the Department of Homeland

Security with responding to the still languishing recommendations of the EMP Commission. The Department of Defense did issue a response, as mandated by the legislation which originally created that Commission. But no such mandatory response was levied at the time on the Department of Homeland Security, which did not even exist when the Commission legislation was passed as part of the National Defense Authorization Act of 2001. The DHS should be required to explain which recommendations they concur with and/or with which they non-concur, and why. They should be asked to prioritize amongst the seventy five and come back with implementation recommendations, or explain why they think it is unnecessary. And finally, I would also urge the Committee to support passage of the Critical Infrastructure Protection Act.

I wish to thank the Committee for this opportunity to present my views of this most important issue.

Testimony of Chris Beck

Vice President for Policy and Strategic Initiatives,

Electric Infrastructure Security Council

For the

Subcommittee on Cybersecurity, Infrastructure Protection,

and Science and Technology

May 8, 2014

Introduction

Good afternoon Chairman Meehan, Ranking Member Clarke, and Members of the Subcommittee. Thank you for holding this hearing on one of the most significant threats to our National and Homeland Security. As many of you know, before I joined EIS Council, I worked for this committee, focusing on Critical Infrastructure Protection and Science and Technology issues. It was through that work that I first became aware of the threats facing our critical electric infrastructures, and I found the issue to be so important that I felt compelled to focus on it exclusively.

The Electric Infrastructure Security Council's mission is to work in partnership with government and corporate stakeholders to host national and international education, planning and communication initiatives to help improve infrastructure protection against electromagnetic threats (e-threats) and other hazards. E-threats include naturally occurring geomagnetic disturbances (GMD), high-altitude electromagnetic pulses (HEMP) from nuclear weapons, and non-nuclear EMP from intentional electromagnetic interference (IEMI) devices – the focus of today's hearing.

EMP - Defining the Issue

The Problem: Developed nations are vulnerable to serious national power grid disruption from e-threats, both natural and malicious.

The Severity: The impact can range from a broad regional blackout with serious economic consequences to, in the worst case, a catastrophe that would threaten societal continuity. With even the most benign scenarios projecting high societal costs, the Committee is correct to focus on this as an issue deserving serious attention.

The Timing: For severe space weather, the most recent events occurred roughly 90 and 150 years ago, but the timing of the next such occurrence, as with all extreme natural disasters, is unknown. Either local (non-nuclear) or sub-continental (nuclear) EMP could occur at any time, encouraged by ongoing vulnerability, and triggered by changing geopolitical realities.

Key Questions

1. **What should our national strategy be?** At top level, there are two alternative paths:

   a. Hope for the best: Accept the status quo.
      i. For severe space weather, this means hoping the most optimistic projections will turn out to be correct, and the impact will not be catastrophic.
      ii. EMP has been called, "The most powerful asymmetric weapon in history." This approach means hoping no terrorist organization or rogue state will ever take advantage of the power of such devastating weapons.

   b. The other alternative:

   Encourage cost-effective resilience, restoration and response planning.

2. **If we respond, what is the path?**
How should we address interconnect-wide interdependence, and how should we proceed with implementation?

3. **If we respond, who should be involved?**
Who should take responsibility to define the path, and implement it? How should the balance between public mandates and private, corporate initiative be determined?

4. **How broad should our response be?**
Should both GMD and EMP be included?

Consensus Recommendations

1. **Hope vs Preparation: Choosing a strategy.**

A common theme of all the many government reports studying these risks, also reflected in the deliberations of the Electric Infrastructure Security Summits over the last several years, is that the risks associated with severe e-threats are serious. It is hard to find anyone who would assert that, in today's world, "hoping for the best" is a good strategy for GMD, EMP or IEMI.

2. **What is the path?**

Our national power grid is organic in design, but administratively complex. This means approaches are needed that address both of these factors.

- Organization and coordination: Given the grid's organic design, the consensus of government studies is that coordinated planning and standards will be important. Finding the best possible balance between broadly accepted, pro-active corporate coordination and government action will be important to assure fast, effective progress in achieving an e-threat resilient grid.

- Technical: A key point, not always recognized, is there is no need to "gold plate" the system.

  For Severe Space Weather, there is already growing discussion of a range of strategies, and none of the approaches under active discussion – from planning measures to comprehensive automated hardware protection – appear high in cost, relative to existing logistics budgets and investment models.

  For EMP, protection planning can focus – not on hardening every component in the power grid – but on protection of a fraction of grid facilities and hardware. In other words, enough resilience investment, and associated restoration planning, to protect enough generation resources and critical loads to allow for both effective restoration and for prioritized support to critical users and installations.

2. Who should be involved?

Given the likelihood of a large regional power outage after a natural or malicious e-threat, power companies will need to be operating in an environment of extensive response and recovery support from federal and state government authorities, as well as community-response NGOs. Thus, the evolution of planning to address these concerns should include the broadest possible involvement of all of these stakeholders, each contributing in its own domain of authority and expertise.

3. How broad should our scope be?

For all the E-threats under consideration here, efforts at protection, if they are to be effective, must primarily be focused where the impact will occur – in the power grid. For severe space weather, there is clearly no other alternative. For malicious threats, EMP and IEMI, U.S. and allied government security officials and experts at the highest levels agree that neither deterrence nor active military measures can alone guarantee the security of our homeland against a determined aggressor prepared to use such weapons.

In conclusion, I should note that there appear to be no significant technical or financial barriers to mitigating this threat. The technologies and operational procedures needed are well understood, and the cost – based on both government estimates and recent corporate experience – is reasonable. One of the primary needs is for education to increase

awareness and therefore willingness to address the problem, and for coordination to address the administrative complexity of our nation's power grid.

This summary of consensus-based themes and recommendations reflects, I believe, not only the conclusions of the many major government studies of these issues, but also the deliberations of the past four international Electric Infrastructure Security Summits, with participation by the highest levels of many departments and agencies of the U.S. and allied governments, and of a broad range of scientists and domain experts working in this field

I would welcome the opportunity to discuss any of these points in greater detail.

This concludes my prepared testimony, and I would be happy to answer any questions.